The National Cyber Security Bill 2024
Heads of Bill

Contents

Part 1- Preliminary and General

Head 1- Short title and commencement

To provide that -

(1) This Act may be cited as the National Cyber Security Act 2024.

(2) This Act shall come into operation on such day as the Minister for Environment, Climate and Communications may appoint by order.

Explanatory Note:
This Head provides for the short title of the proposed Act and makes provision for its commencement whether in full or in part.

Head 2- Definitions

To provide that –

(1) "In this Act,

'management board' means a body of group of individuals vested with the authority and responsibility for the oversight, direction and control of an entity.

'cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;

'Commission' means the European Commission;

" 'ComReg' means the Commission for Communications Regulation established by Part 2 of the Communications Regulation Act 2002;".

'competent authority' means the person designated as a competent authority in the State under Head 17

"Cooperation Group" means the Cooperation Group as defined in Directive (EU) 2016/1148 of The European Parliament and Of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

'content delivery network' means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;

'CSIRT' has the meaning assigned to it by Head 12;

"CSIRT in another member state" means any authority or body designated as a computer security incident response team by a member state (other than the State) for the purposes of the Directive;

'CSIRTs network' means the network of national computer security incident response teams referred to in Article 12 of the Directive;

'cybersecurity' means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;

'cyber threat' means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

'data centre service' means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;

['Data Protection Regulation' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 20162 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation);]

'digital service' means a service as defined in Article 1(1), point (b), of Directive (EU) 2015/1535 of the European Parliament and of the Council (30);

“Directive” means DIRECTIVE (EU) 2022/2555 of the European Parliament and Of The Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive);

‘Domain Name System (DNS) abuse’ is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.

‘domain name system’ or ‘DNS’ means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources;

‘DNS service provider’ means an entity that provides:
(a) publicly available recursive domain name resolution services for internet end-users; or
(b) authoritative domain name resolution services for third-party use, with the exception of root name servers;

‘electronic communications service’ means an electronic communications service as defined in Article 2, point (4), of Directive (EU) 2018/1972;

‘entity’ means a natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;

“enactment” means—
(a) an Act of the Oireachtas,
(b) a statute that was in force in Saorstát Éireann immediately before the date of the coming into operation of the Constitution and that continues in force by virtue of Article 50 of the Constitution, or
(c) an instrument made under an Act of the Oireachtas or a statute referred to in [section (b)];

‘ENISA’ means the European Union Agency for Cybersecurity

‘entity providing domain name registration services’ means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller;

‘EU-CyCLONe’ means the European cyber crisis liaison organisation network, as established pursuant to Article 16 of the Directive.

‘ICT product’ means an element or a group of elements of a network or information system;

‘ICT service’ means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;

‘ICT process’ means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service

‘incident’ means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;

‘incident handling’ means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident;

‘internet exchange point’ means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;

‘large-scale cybersecurity incident’ means an incident which causes a level of disruption that exceeds a Member State’s capacity to respond to it or which has a significant impact on at least two Member States;

‘managed service provider’ means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers’ premises or remotely;

‘managed security service provider’ means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management;

‘Minister’ means Minister for the Environment, Climate and Communications;

“National Cyber Security Centre” is an operational cybersecurity unit within the Department of the Environment, Climate and Communications. It is the primary Cyber Security authority in the State, responsible for leading the national response to cyber security incidents and shall also be referred to as the NCSC;

‘national cybersecurity strategy’ means the national strategy prepared by the Minister under Head 24;

‘near miss’ means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise;

‘network and information system’ means:

(a) an electronic communications network that means transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

‘online marketplace’ means a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers;

‘online search engine’ means a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found;

‘Open Systems Interconnection Model’ provides a common basis for the coordination of standards development for the purpose of systems interconnection, while allowing existing standards to be placed into perspective within the overall Reference Model

‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

‘prescribed’ means prescribed by regulations made by the Minister under this [Act];

‘public administration entity’ means an entity recognised as such in the State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria:

(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) it has legal personality or is entitled by law to act on behalf of another entity with legal personality;

(c) it is financed, for the most part, by the State, regional authorities or by other bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities or by other bodies governed by public law;

(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital;

‘public body’ means:

a) a local authority within the meaning of the Local Government Act 2001;
b) a university within the meaning of the Universities Act 1997;
c) any other person, body or organisation established—
    a. by or under an enactment (other than the Companies Acts) or charter,
    b. by any Scheme administered by a Minister of the Government, or
    c. under the Companies Acts in pursuance of powers conferred by or under another enactment, and financed wholly or partly by means of money provided, or loans made or guaranteed, by a Minister of the Government or the issue of shares held by or on behalf of a Minister of the Government,
d) a company (within the meaning of the Companies Acts) a majority of the shares in which are held by or on behalf of a Minister of the Government,
e) any other person, body, organisation or group financed wholly or partly out of moneys provided by the Oireachtas that stands prescribed for the time being (being a person, body, organisation or group that, in the opinion of the Minister, following consultation

with the Commission, ought, in the public interest and having regard to the provisions and spirit of this Act, to be prescribed);

'public electronic communications network' means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services which support the transfer of information between network termination points;

'qualified trust service' means a qualified trust service as defined in Article 3, point (17), of Regulation (EU) No 910/2014;

'qualified trust service provider' means a qualified trust service provider as defined in Article 3, point (20), of Regulation (EU) No 910/2014;

'representative' means a natural or legal person established in the Union explicitly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the Union, which may be addressed by a competent authority or a CSIRT in the place of the entity itself with regard to the obligations of that entity under the Directive;

'research organisation' means an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions.

'risk' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems;

'significant cyber threat' means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage;

'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations;

'standard' means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory, and which is one of the following:

(a) 'international standard' means a standard adopted by an international standardisation body;

(b) 'European standard' means a standard adopted by a European standardisation organisation;

(c)‘harmonised standard’ means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation;

(d) ‘national standard’ means a standard adopted by a national standardisation body;

‘technical specification’ means a document that prescribes technical requirements to be fulfilled by a product, process, service or system and which lays down one or more of the following:

a) the characteristics required of a product including levels of quality, performance, interoperability, environmental protection, health, safety or dimensions, and including the requirements applicable to the product as regards the name under which the product is sold, terminology, symbols, testing and test methods, packaging, marking or labelling and conformity assessment procedures;
b) production methods and processes used in respect of agricultural products as defined in Article 38(1) TFEU, products intended for human and animal consumption, and medicinal products, as well as production methods and processes relating to other products, where these have an effect on their characteristics;
c) the characteristics required of a service including levels of quality, performance, interoperability, environmental protection, health or safety, and including the requirements applicable to the provider as regards the information to be made available to the recipient, as specified in Article 22(1) to (3) of Directive 2006/123/EC;
d) the methods and the criteria for assessing the performance of construction products, as defined in point 1 of Article 2 of Regulation (EU) No 305/2011 of the European Parliament and of the Council of 9 March 2011 laying down harmonised conditions for the marketing of construction products (37), in relation to their essential characteristics;

‘top-level domain name registry’ or ‘TLD name registry’ means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use;

‘trust service’ means a trust service as defined in Article 3, point (16), of Regulation (EU) No 910/2014;

‘trust service provider’ means a trust service provider as defined in Article 3, point (19), of Regulation (EU) No 910/2014;

‘vulnerability’ means a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat;

Explanatory Note:

This Head provides for the definitions used in the Bill, most of which are taken from Article 6 of the Directive (Eu) 2022/2555 Of The European Parliament And Of The Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

This Head also includes additional definitions, such as for the Minister and for the National Cyber Security Centre.

PART 2- The National Cyber Security Centre

Head 3- The National Cyber Security Centre

(1) The National Cyber Security Centre (NCSC), which is under the authority of the Minister, and, subject to subsection (3) below, its functions are to—

a. protect and defend the security and integrity of network and information systems in the State, including by monitoring and analysing risks and threats and by cooperating with relevant authorities within and outside the State,
b. respond to network and information security incidents in the State
c. produce Reports on National Security risks and incidents for the Minister and the Taoiseach.
d. deny the use of network and information systems in the State to acts of foreign or domestic interference that are, or are intended to be, detrimental to the interests of the State or its international relations or are clandestine or deceptive or involve a threat to any person, device or essential service.
e. assist with the security and integrity of electronic communications services in the State.
f. monitor the security of Government network and information systems and communications technology, including mobile communications and electronic communications.,
g. provide support and assistance to the Defence Forces and An Garda Siochana in relation to protecting the State from unlawful acts that subvert or undermine, or are intended to subvert or undermine, parliamentary democracy or the institutions of the State,
h. provide support and assistance to An Garda Siochana, in relation to the prevention or detection of serious crime. including, where necessary, the sharing of information under [Head 11].
i. collect and analyse technical information related to network and information security and to provide information and advice about threats and incidents relating to the network and information systems to Government, critical infrastructure operators and the general public.
j. develop initiatives and strategies to assist in the development of the cyber security industry in Ireland.
k. monitor and identify foreign information manipulation and interference.

(2) The NCSC shall have all such powers as are necessary or expedient for the performance of its functions.

(3) Nothing in this [Act] shall prejudice the ability of the State to safeguard its essential functions, in particular its national security, including taking action to protect information the disclosure of which is considered by the NCSC or any competent authority designated under this Act to be contrary to the State's essential security interests, the maintenance of law and order and, in particular, the investigation, detection and prosecution of criminal offences.

Explanatory Note:
The NCSC was established by Government Decision in July 2011 with a broad remit across the cyber security of Government ICT and critical national infrastructure. This included a national incident response capability, international cooperation and engaging with critical

infrastructure operators. Under Regulation 10 of S.I. 360 of 2018, the Computer Security Incident Response Team (or CSIRT) within the NCSC was designated as the national CSIRT. The NCSC has subsequently been assigned a number of other roles, including as National Coordination Centre under Regulation (EU) 2021/887, and as National Cybersecurity Authority under Regulation (EU) 2019/881.

The National Cyber Security Strategy 2019-2024 is a whole-of-Government approach to address the growing threat of cyber security incidents and to ensure that Ireland can benefit fully from the digital transformation. The strategy includes 20 separate measures to safeguard public sector networks and essential services, to facilitate the development of the cyber security industry and to promote awareness raising and international cooperation.

As part of the implementation of the strategy, early in 2021 external consultants were commissioned to conduct a Capacity Review and to benchmark the NCSC with similar agencies in Europe and internationally. The report on the Capacity Review was received in June 2021. In July 2021 the Government agreed a number of measures to support the continued development of the NCSC over the coming five years.

The measures agreed included that a General Scheme of a Bill be prepared for Government approval to establish the NCSC on a statutory basis and provide for related matters, including clarity around its mandate and role and in relation to other actors in the cyber area.

This Head provides for establishment on a legislative basis of the National Cyber Security Centre (NCSC) on a statutory basis as an Executive Office of the Minister and the Department for Environment, Climate and Communications. Because the organisation has a series of National Security roles it cannot be fully independent of Ministerial Authority. On that basis, it is being established as an executive office within the Department, with reporting obligations to the Minister and to the Oireachtas.

The Head provides for a set of roles for NCSC including national cyber security monitoring, the incident response function, resilience building, information sharing (national and international), national incident response. While some of this is premised on the ensuring that the general roles foreseen under NIS2 can be met, the Head is primarily aimed at giving the NCSC a comprehensive legal basis to conduct the existing and developing set of roles that bodies of this type have internationally.
Under the NIS 2 Directive, teams within the NCSC or the NCSC itself will hold the following functions:

- Designated Competent Authority for certain entities (as agreed by Government decision on the 20/12/2023))
- Designated Cyber Crisis Management Authority
- Single Point of Contact on cybersecurity (SPOC)
- Computer Security Incident Response Team (CSIRT)

This Head provides for the appointment and role of the Director of the NCSC. The NCSC was established in 2011. A Director was appointed to the role in January 2022 and is currently in situ.

The operations of the NCSC shall be under the control of a Director appointed by the Minister.

Head 4- Directions of Minister

(1) The Minister may give general directions in writing to the NCSC for any purpose in relation to the functions of the NCSC under this Act or for any other purpose in relation to the provisions of this [Act], or any other enactment.

(2) The Minister may, by order, assign additional tasks or responsibilities to the NCSC as the Minister considers to be incidental to or consequential on the functions assigned to them under other provisions of this Part.

(3) The Minister may direct the NCSC to supply the Minister with information, reports or [other data], in the manner and within the period, both as the Minister may determine, in relation to the performance by the NCSC of its functions under this [Act].

(4) The Minister may, in relation to the performance by the NCSC of its functions under this [Act], give a direction in writing to the NCSC requiring it to comply with such policies of the Government as are specified in the direction.

(5) The Minister may, by direction in writing, amend or revoke a direction under this section (including a direction under this subsection).

(6) The NCSC shall comply with a direction under this section.

Explanatory Note:

This Head provides for a policy choice for the Minister to make certain directions to the NCSC under this Act that must be complied with (which he may later revoke or amend)

These include the supply of information, reports or [other data], in relation to the performance by the NCSC of its functions under this [Act] or requiring their compliance with such policies of the Government as are specified in the direction.

Head 5 – Guidelines of the Minister

(1) For the purpose of providing practical guidance as regards compliance by essential or important entities with their obligations under this [Act], the Minister may, from time to time and following consultation with such persons (if any) as he or she considers appropriate, issue guidelines.

(2) Before issuing guidelines under this [Act], the Minister shall publish a draft of the proposed guidelines and shall give persons a period of 30 working days from the date of the publication of the draft within which to make written representations to him or her in relation to that draft.

(3) The Minister may, having considered any relevant representations received under subsection (3), issue the guidelines with or without modification.

(4) The guidelines shall specify the date on which they are to come into operation.

(5) The Minister may, following consultation with such persons (if any) as he or she considers appropriate, amend or revoke guidelines published under this [Act].

(6) The Minister shall publish the guidelines and, where they have been amended, the guidelines as so amended.

Explanatory Note:

This Head is a policy choice to allows the Minister to issue national guidelines for the purpose of providing practical guidance as regards compliance by essential or important entities with their obligations under this [Act],

Head 6 – Scanning

(1) The NCSC may carry out proactive non-intrusive scanning of publicly accessible network and information systems in the State, including of essential and important entities.
(2) Such scanning shall only be carried out to detect vulnerable or insecurely configured network and information systems and to inform the entities concerned.
(3) When carrying out the tasks referred to in the first subparagraph, the NCSC may prioritise particular tasks on the basis of a risk-based approach.
(4) The NCSC may conduct offensive assessments of publicly accessible network and information systems in the State, including of essential and important entities, with the consent of the entities in question.

Explanatory Note:

This Article is designed to give the NCSC specific powers to engage in a range of scanning type activities. This type of activity is widely conducted by bodies working in Cyber Security, and for the very most part does not interfere with the subject systems. The NCSC would use this type of scanning to identify systems vulnerable to specific exploits, or in some cases, those that are subject to active compromise. It is possible, albeit unlikely, that this type of scanning would also identify infrastructure in the State that was in use by a threat actor, without the knowledge of the owner of said infrastructure.

Under NIS2, as regards personal data, the CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679, upon the request of an essential or important entity, a proactive scanning of the network and information systems used for the provision of the entity's services.

This type of activity is also required of the State under Article 11 of NIS2 , where CSIRTs shall provide, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;. Also, several provisions (including Articles 2-6) of the Criminal Justice (Offences Relating to Information Systems) Act 2017 prohibit certain types of activity without lawful authority; this and several other elements of this legislation are to provide said authority.

Head 7 – DNS Blocking and Sinkholing

(1) When it becomes aware of a pressing National Security threat likely to undermine the security of the information systems of the Public Authorities or Essential Entities as referred to in Head X of this Bill, the NCSC may:

(2) When the NCSC determines that domain name abuse poses a risk to national security or to the security of network and information systems in the State, the NCSC may ask a DNS Service Provider or domain registrar to take appropriate measures to this threat within a period of time that it sets and which takes into account the nature of the threat.

(3) The types of abuse referred to in the first sub paragraph includes, but not limited to;
   a. Malware distribution;
   b. Botnet Attacks;
   c. Distributed Denial of Service Attacks;
   d. Unauthorised changes to DNS entries which result in users being redirected to a spoofed, malicious website rather than the legitimate site they were attempting to reach, and
   e. Spam (when it is used to deliver other forms of DNS Abuse).

(4) If this threat has not been neutralised within the prescribed period, the NCSC may request a domain name resolution system operator, to take such actions as required to terminate the DNS abuse.

Explanatory Note:

This section aims to establish a system to allow the NCSC to take a number of different measures in specific cases where the Domain Name System (DNS) system is being abused or compromised by a threat actor in order to perpetuate harm against systems in Ireland or elsewhere. The DNS is the so called 'phone book' of the internet, and essentially interpolates between the domain name hierarchy and the Internet Protocol Address space. Threat actors, meaning States and Criminal Actors, can misuse the DNS in a number of ways, including to compromise traffic to critical infrastructure and to conduct denial of service attacks (so called distributed denial of service, or DDOS attacks). The State has seen a significant number of these incidents in the period since February 2022.

This is a dynamic area, where threat actors continually evolve and develop new methodologies and so the measures contained in this Head are flexible so as to allow a National response to changing circumstances. Also, in many cases these incidents have complex international elements, whereby the origin of the incident and the target may be in different jurisdictions. As such, these powers are necessary to ensure that the territory of this State is not used as a base for offensive action against other States.

These powers include basic powers to block or suspend certain domains where abuse is determined to have occurred, along with restrictions on their use.

In Recital 126 of NIS2, it states that in duly substantiated cases where it is aware of a significant cyber threat or an imminent risk, the competent authority should be able to take immediate enforcement decisions with the aim of preventing or responding to an incident.

Head 8 – Sensor Employment on Networks of Essential and Important Entities

(1) With the consent of the entities concerned, the NCSC may deploy, on the network of organisations in the State:
    a. devices or software to collect metadata and data, to include source and destination of IP address traffic or volumes of data.
    b. or, on the devices of public sector bodies, devices or software allowing the collection of all traffic data.
(2) These measures shall be implemented only to the extent strictly necessary for the detection and management of threat and risks to network and information security.
(3) Individually designated and specially authorised officials of the NCSC shall be authorised, for the sole purpose of preventing and characterising the threat affecting the information systems of the entities referred to in the first subparagraph of this article, to collect data and analyse only the relevant technical data, to the exclusion of any other exploitation.
(4) Data collected by these means may not be retained for more than 18 months and the destruction of all of these data must be certified by the NCSC to the High Court.

Explanatory Note:

The purpose of this head is to allow for the NCSC, with the consent of entities concerned, to deploy sensors onto the corporate networks of essential and important entities.

Sensor involves placing a physical device on the network of a potential victim and using that to monitor certain types of traffic entering and exiting that network. The technology underpinning this will change, and it is likely that over time it will be replaced by some form of non-physical software-based system. There are a range of information processing powers required, both under NIS2 and to meet specific national security requirements.

The existing Sensor network operated by the NCSC is limited to Government entities. There is a longstanding requirement to offer the deployment of a sensor or sensorlike capabilities to other entities in the State in order to manage national security risks to key infrastructure or services. The most effective way of doing this is to provide for the NCSC to be able to deploy a sensor to any entity within the State that consents to doing so (subject to the completion of a DPIA, as is the case already), regardless of whether they are covered by NIS2.

These sensors, which are already in use across Government, are used to track DNS connections made to and from users within the network. This allows the NCSC to identify certain high-level risks and threats as they occur and to detect and, in some cases, prevent cyber security incidents.

These devices will be placed voluntarily on the networks of some essential and important entities.

Critically it is also proposed to be able to retain all traffic data crossing government networks for up to 18 months. This is to facilitate the retrospective identification and mapping of threats after activity in and on government infrastructure in Ireland. This type of system is critical in allowing the NCSC to conduct its functions, and particularly in detecting and properly responding to national security risks.

Head 9 – Temporary Sensor Employment on Communications Networks

(1) When it becomes aware of a pressing National Security threat likely to undermine the security of the information systems of the Essential Entities essential public administration entities or as referred to in [Heads 21 and 23] of this [Act], the NCSC may:

(2) Deploy devices to collect corresponding to Layers 1-4 inclusive of the Open Systems Interconnection Model on the network of a provider of public communications networks and publicly available electronic communications services or of a data centre operator

(3) (b) request specific traffic data corresponding to Layers 1-4 inclusive of the Open Systems Interconnection Model from providers of public communications networks and publicly available electronic communications services or from data centre operators.

(4) The NCSC may only apply devices at (a) or (b) on the basis of an application to the High Court which shall—
    a) be made ex parte,
    b) be upon information on oath specifying the grounds on which the order is sought,
    c) specify the period of time for which retention of Schedule 2 data by service providers is, in the view of the NCSC, required for the purposes of safeguarding the security of the State.

(5) If the High Court is satisfied, on an application by the NCSC, that the hearing of an application under section (2) is likely to result in the disclosure of relevant material and that such disclosure would create a risk to the security of the State it shall exclude from the hearing of the appeal all persons except—
    a) a judge hearing the matter,
    b) a judicial assistant, or other court personnel, whose presence is necessary for the judge to hear the matter,
    c) the parties to the proceedings,
    d) the legal representatives of the parties to the proceedings, and
    e) a witness whose evidence is relevant to the proceedings, for as long as the witness's presence is required for the purpose of providing such evidence, unless it is satisfied that the interests of justice require any other person not to be so excluded.

(6) The High Court shall grant the order applied for under subsection (2) if it is satisfied that -

(7) the NCSC has grounds for believing that there are real and present risks to the security of the State, or

(8) the NCSC has grounds for believing that there are real and present risks to the security of the State or the confidentiality, integrity or authenticity of public sector data or to the continuity of Essential Services

(9) The order granted under section (2) shall be implemented for a limited period of time and shall be implemented to an extent strictly necessary for the detection and management of threat and risks to network and information security.

(10) The cessation of the use of the order granted under section (2) must be recorded to the same judge of the High Court referred to in section (2).

(11) Individually designated and specially authorised officials of the NCSC shall be authorised, for the sole purpose of preventing and characterising the threat affecting the information systems of the entities referred to in the first subparagraph of this article, to collect data and analyse only the relevant technical data, to the exclusion of any other exploitation.

(12) Data collected by these means may not be retained for more than six months and the destruction of all of these data must be certified by the NCSC on application to the High Court.

Explanatory Note:

There are a range of information processing powers required, both under NIS2 and to meet specific national security requirements.
The existing Sensor network operated by the NCSC is limited to Government entities. There is a longstanding requirement to offer the deployment of a sensor or sensorlike capabilities to other entities in the State in order to manage national security risks to key infrastructure or services. The most effective way of doing this is to provide for the NCSC to be able to deploy a sensor to any entity within the State that consents to doing so (subject to the completion of a DPIA, as is the case already), regardless of whether they are covered by NIS2.

These powers are to be used in extremis to allow the extension of the NCSC's existing sensor network on a temporary and very limited basis to telecommunications and data centre operations in the State.
In practical terms, this would involve either the fitting of physical or virtual devices on the networks of telecommunications and data centre operations **on a very temporary basis** to monitor potential national security risks.

Given the sensitivity of the data, ensuring the secure, limited and proportionate use of these tools is essential. Parts 2 – 6 of this make provision for independent judicial oversight, the means by which these data can be held, analysed and must be destroyed, as well as limits on storage.

Head 10 – Processing of Personal Data

(1) The NCSC may process personal data for purposes other than those for which the data were originally collected, without prejudice to Article 6(4) of Data Protection Regulation [and the Data Protection Act 2018], if the processing is necessary.
    a. to collect, evaluate or investigate information on security risks or security precautions for information technology, or
    b. for support, advice or warning in questions of security in information technology and
    c. for reasons of National Security

and there is no reason to assume that the legitimate interest of the data subject takes precedence.

(2) Under Article 9(2)(g)) of [Act] (EU) 2016/679 and without prejudice to [section 45 Data Protection Act 2018], the processing of special categories of personal data by the NCSC is permissible if:
    a. the processing is necessary to avert a significant threat to network, data or information security,
    b. an exclusion of this data from processing would make the fulfilment of the tasks of the NCSC impossible or significantly endanger them,

and there is no reason to assume that the legitimate interest of the data subject in the exclusion of this data from processing prevails.

(3) The NCSC shall provide for appropriate and specific measures to safeguard the interests of the data subject in accordance with [section 36 Data Protection Act 2018].

Explanatory Note:

This Head provides for the legal basis for the NCSC to process personal data. The NCSC has an operational requirement to collect, process, store and share a range of personal information. Some of this requirement flows from the general work of the organisation in detecting and defeating cybersecurity incidents in the State, including those with a national security component.

Article 6(1)(f) of the General Data Protection Regulation permits the processing of personal data to the extent that such processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. The Cyber Security Bill will include heads that deal with information sharing by a competent authority, the CSIRT or the single point of contact in relation to an essential and important entities or DSP, as required by the Directive, as well as explicit national security roles for the NCSC. These heads will permit information sharing with AGS, DF or DPC, and may in some limited circumstances contain personal data (particularly where files or documents being examined themselves contain personal data).

Article 6(1)(f) of the General Data Protection Regulation permits the processing of personal data to the extent that such processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. The legitimate interest ground shall not apply to processing carried out by public authorities in the performance of their tasks. However, the European Commission has confirmed its view that the said restriction should be interpreted as applying only to situations where the public authority is acting in its capacity as a public authority.

By contrast, where the public authority is acting in another capacity, for instance where it is acting in its capacity as employer, owner/occupier of property, or as the operator of an internal computer network, the public authority is entitled to rely upon the legitimate interest ground in the same way and to the same extent as any other data controller or processor.

Central Government, in its capacity as employer and operator of an internal computer network, is entitled to rely upon the public interest ground as a legal basis for implementing necessary measures to ensure network and information security.

Recital (121) of the Regulation which provides that the processing of personal data, to the extent necessary and proportionate for the purpose of ensuring security of network and information systems by essential and important entities, could be considered to be lawful on the basis that such processing complies with a legal obligation to which the controller is subject, in accordance with the requirements of Article 6(1), point (c), and Article 6(3) of Regulation (EU) 2016/679.

This Recital further states that the processing of personal data could also be necessary for legitimate interests pursued by essential and important entities, as well as providers of security technologies and services acting on behalf of those entities, pursuant to Article 6(1), point (f), of Regulation (EU) 2016/679, including where such processing is necessary for cybersecurity information-sharing arrangements or the voluntary notification of relevant information in accordance with this Directive. Measures related to the prevention, detection, identification, containment, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated vulnerability disclosure, the voluntary exchange of information about those incidents, and cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools could require the processing of certain categories of personal data, such as IP addresses, uniform resources locators (URLs), domain names, email addresses and, where they reveal personal data, time stamps.

Processing of personal data by the competent authorities, the single points of contact and the CSIRTs, could constitute a legal obligation or be considered to be necessary for carrying out a task in the public interest or in the exercise of official authority vested in the controller pursuant to Article 6(1), point (c) or (e), and Article 6(3) of Regulation (EU) 2016/679, or for pursuing a legitimate interest of the essential and important entities, as referred to in Article 6(1), point (f), of that Regulation. Furthermore, national law could lay down rules allowing the competent authorities, the single points of contact and the CSIRTs, to the extent that is necessary and proportionate for the purpose of ensuring the security of network and information systems of essential and important entities, to process special categories of personal data in accordance with Article 9 of Regulation (EU) 2016/679, in particular by providing for suitable and specific measures to safeguard the fundamental rights and interests of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy- preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

This Head provides for the NCSC, as part of central government, to be able to process data for purposes other than those for which the data were originally collected, if necessary to collect, evaluate or investigate information on security risks or security precautions for information technology; for support, advice or warning in questions of security in same; and for reasons of National Security.

There are data processing concerns that may arise where the NCSC is accessing and monitoring data, where national security is not directly in issue. In these cases, (where the data is used for

purposes other than ‘national security, ensuring network and information security or in relation to potential criminal acts’, then the NCSC must ensure there is a legal basis for the processing of any personal data and that the principles relating to processing of personal data are adhered to (Article 5 GDPR).

Head 11 – Sharing Information and Co-operation with Data Protection Commission and the Garda Síochána

(1) Information, including personal data may be shared by a competent authority or the NCSC as the single point of contact where required to fulfil the requirements of this Act.

(2) Information shared in accordance with this Act may include personal data.

(3) Where a competent authority or the NCSC as the single point of contact shares information under this Act in relation to an essential or important entity at set out in Schedule I and II, the competent authority or the NCSC as the single point of contact , as the case may be, shall take all reasonable steps to protect the confidentiality of the information so shared and the network and information security and commercial interests of the essential or important entity to which the information relates.

(4) The NCSC as the single point of contact and the competent authority shall consult and co-operate with, including, where necessary, by sharing information with, the Data Protection Commission where the Data Protection [Act] or the Data Protection Acts 1988 to 2018 apply in relation to any matter concerning this [this Act], including in relation to an incident resulting in a personal data breach in which case the competent authority shall work in close co-operation with the Data Protection Commission in addressing the incident.

(5) The NCSC as the single point of contact and the competent authority shall consult and co-operate with, including, where necessary, by sharing information with, the Garda Siochána in relation to any matter to which this Act applies.

Explanatory Note:

This Head contains provisions taken from S.I. 360 of 2018 and provides for the sharing of information between the NCSC as the CSIRT with other public bodies in accordance with this Act.

By far the most common type of information that the NCSC shares are so called 'Indicators of Compromise' (or IOCs). This is the collective term used for a variety of different types of information used as evidence of potential intrusions on a system or network. The NCSC regularly shares these IOCs with partners domestically and internationally, and in some case publishes these as part of general advisories, warnings or notifications to the public.

Part 3- The Network and Information Systems Directive

Head 12 – Computer Security Incident Response Team (CSIRT): Requirements and Tasks

(1) The NCSC is for the purposes of this Act designated as the Computer Security Incident Response Team, also known as a CSIRT, which shall:
   a. comply with the requirements set out in Head 16(1) of this Act, shall cover at least the sectors, subsectors and types of entity referred to in Schedule I and II, and shall be responsible for incident handling in accordance with a well-defined process;
   b. utilise appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholder contribute to the deployment of secure information-sharing tools;
   c. cooperate and, where appropriate, exchange relevant information in accordance with Head 33 with sectoral or cross-sectoral communities of essential and important entities;
   d. participate in peer reviews organised in accordance with Article 19 of the Directive, and provide effective, efficient and secure cooperation within the CSIRTs network; and
   e. notify the Commission regarding its designation as CSIRT and coordinator pursuant to Head 16(1) of this Act of its respective tasks in relation to essential and important entities, and of any subsequent changes thereto.

(2) The CSIRT may:
   a. participate in international cooperation networks and establish cooperation relationships with third countries' national computer security incident response teams, where they shall facilitate effective, efficient and secure information exchange with those third countries' national computer security incident response teams, using relevant information-sharing protocols, including the traffic light protocol;
   b. exchange relevant information with third countries' national computer security incident response teams, including personal data in accordance with Union data protection law; and
   c. cooperate with third countries' national computer security incident response teams or equivalent third-country bodies, in particular for the purpose of providing them with cybersecurity assistance.

(3) The CSIRT shall comply with the following requirements:
   a. ensure a high level of availability of their communication channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times by clearly specifying the communication channels and make them known to constituency and cooperative partners;
   b. locate the CSIRT premises and the supporting information systems at secure sites;
   c. have an appropriate system for managing and routing requests, in particular to facilitate effective and efficient handovers;
   d. ensure the confidentiality and trustworthiness of their operations;
   e. be adequately staffed to ensure availability of their services at all times and ensure that their staff are trained appropriately; and
   f. are equipped with redundant systems and backup working space to ensure continuity of their services.

(4) The CSIRT shall undertake the following tasks:

a. monitor and analyse cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;
b. provide early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;
c. respond to incidents and providing assistance to the essential and important entities concerned, where applicable;
d. collect and analyse forensic data and provide dynamic risk and incident analysis and situational awareness regarding cybersecurity;
e. provide, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;
f. participate in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;
g. where applicable, act as a coordinator for the purposes of the coordinated vulnerability disclosure under Head 16 (1) of this Act;
h. contribute to the deployment of secure information-sharing tools pursuant to [section 1(b)]
i. When carrying out the tasks referred to in [section 4], the CSIRT may prioritise particular tasks on the basis of a risk-based approach.

(5) The CSIRT may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential and important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned.

(6) The CSIRT shall establish relationships with relevant stakeholders in the private sector, with a view to achieving the objectives of this Act by promoting the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to:
a. incident-handling procedures;
b. crisis management; and
c. coordinated vulnerability disclosure under Head 16(1).

Explanatory Note:

This Head transposes Articles 10 and 11 of the NIS2 Directive.

Under Article 10, Member States are required to establish or designate one or more Computer Security Incident Response Team (CSIRT) under the NIS2 Directive. The CSIRT's function is to prevent, detect, respond to and mitigate cyber security incidents and risks.

Many of the provisions in Article 10 replicate similar provisions as set out in the NIS Directive which were transposed into Irish law in Section 10 of S.I. 360 of 2018.

Similar to 10 of S.I. 360 of 2018 the Department's policy is that the NCSC will once again act as Ireland's CSIRT for the purposes of the Directive. The Government reaffirmed the NCSC's mandate to act as national cyber incident response in the National Cyber Security Strategy 2019-2024 and the Strategic Emergency Management Framework. The Operations Division in the NCSC will carry out these functions. This unit has achieved international accreditation and its capabilities have been expanded further as part of the National Cyber Security Strategy. The CSIRT currently engages in international cooperation and information exchange with its counterparts in Europe and North America.

The NCSC is already fulfilling the role of CSIRT under S.I. 360 of 2018 in relation to the NIS Directive. This section sets out their responsibilities.

This Head also sets out the specific requirements and tasks the CSIRT is expected to carry out as required by Article 11 of the NIS 2 Directive.

Head 13- Single Points of Contact

(1) The NCSC is designated a single point of contact in the State for the purpose of this Act.
(2) The Single point of contact shall –
    a. liaise with a relevant authority in another member state, the Co-operation Group, the CSIRTs network and, where appropriate, with the Commission and ENISA to ensure cross-border co-operation in relation to this Act; and
    b. co-operate with all the designated competent authorities and the CSIRT in accordance with this Act.
(3) The NCSC shall notify the Commission without undue delay of its designation as the single point of contact referred to in section 1 and of any subsequent changes thereto.

Explanatory Note:
This Head sets out the provisions regarding the designation of a Single Point of Contact as per Article 8 of the NIS2 Directive. The provisions mirror the ones provided for the single point of contact in S.I. 360 of 2018. The other provisions of Article 8 relate to the designation of Competent authorities. These provisions are dealt with in Head 17.

Head 14- National Cyber Crisis Management

(1) The NCSC is for the purposes of this Act designated as the competent authority for the management of large-scale cybersecurity incidents and crises in the State.

(2) Within six months of the entry into force of this Act, the NCSC shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular:
   a. the objectives of national preparedness measures and activities;
   b. the tasks and responsibilities of the NCSC;
   c. the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels;
   d. national preparedness measures, including exercises and training activities;
   e. the relevant public and private stakeholders and infrastructure involved; and
   f. national procedures and arrangements between relevant national authorities.

(3) Within three months of the entry into force of this Act, the NCSC shall notify the European Commission of its role in managing cyber security incidents.

Explanatory Note:

This Head transposes Article 9 of the NIS2 Directive as it relates to the designation of a competent authority for major cyber security incident response processes, including coordinating across Government. It also sets out the requirement for that designated body to adopt a large-scale cybersecurity incident and crisis response plan.

In accordance with the Annex to Recommendation (EU) 2017/1584, a large-scale cybersecurity incident should mean an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States. Depending on their cause and impact, large-scale cybersecurity incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market or posing serious public security and safety risks for entities or citizens in several Member States or the Union as a whole.

Article 9 makes a reference to working with existing emergency and crisis management functions in the state. The relevant system in Ireland, the Strategic Emergency Management system operated by the Office of Emergency Planning in the Department of Defence, does not have a statutory base and so no reference to it is made here. The national plan referred to in (2) will include references to it though, as required by 2(d).

In accordance with Article 9 of the NIS2 Directive, the NCSC is required to adopt a national large-scale cybersecurity incident and crisis response plan within 6 months of the entry into force of this Act.

Head 15- Incident Response Powers/Reporting Obligations

(1) Essential and Important entities shall notify, without undue delay, the CSIRT in accordance with section (3) of any incident that has a significant impact on the provision of their service.

(2) Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services.

(3) Where applicable, essential and important entities shall communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

(4) Sections (1), (2) and (3) shall also apply to public bodies.

(5) An incident shall be considered to be significant if:

   a. it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
   b. it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

(6) For the purpose of notification under section (1), the entities concerned shall submit to the CSIRT:

   a. without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
   b. without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;
   c. upon the request of a CSIRT an intermediate report on relevant status updates;
   d. a final report not later than one month after the submission of the incident notification under point (b), including the following:
   e. a detailed description of the incident, including its severity and impact;
   f. the type of threat or root cause that is likely to have triggered the incident;
   g. applied and ongoing mitigation measures;
   h. where applicable, the cross-border impact of the incident;
   i. in the event of an ongoing incident at the time of the submission of the final report referred to in section (4)(d), entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

(7) By way of derogation from the section (4)(b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT without undue delay and in any event within 24 hours of becoming aware of the significant incident.

(8) The CSIRT shall provide, without undue delay and where possible within 24 hours of receiving the early warning referred to in section (4)(a), a response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. The CSIRT shall provide additional technical support if the entity concerned so requests. Where the significant incident is suspected to be of criminal nature, the CSIRT shall provide guidance on reporting the significant incident to law enforcement authorities.

(9) Where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT shall inform, without undue delay, the other affected Member States and ENISA of the significant incident. Such information shall include the type of information received in accordance with section (4). In so doing, the CSIRT or the single point of contact shall, in accordance with Union or national law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

(10) Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, the CSIRT may, after consulting the entity concerned, inform the public about the significant incident, or require the entity to do so.

(11) At the request of the CSIRT the single point of contact shall forward notifications received pursuant to section (1) to the single points of contact of other affected Member States.

(12) The NCSC, as the single point of contact, shall submit to ENISA every three months a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with section 1 and with Head 34.

(13) The CSIRT shall provide to the competent authorities under Directive (EU) 2022/2557 information about significant incidents, incidents, cyber threats and near misses notified in accordance with section (1) and with Head 34 by entities identified as critical entities under Directive (EU) 2022/2557.

(14) In the case of a cross-border or cross-sectoral significant incident, the CSIRT shall without delay inform the single point of contact the relevant information notified in accordance with section (4).

Explanatory Note:

This Head transposes Article 23 of the NIS 2 Directive. This essentially mirrors section 18 and 22 of S.I. 360 of 2018. Of particular note here is the text at section 3, which establishes new criteria for the significance threshold which triggers an incident notification. This is highly sensitive in any case because of the potential for Ireland to be the notifiable authority in respect of a number of large multinational entities operating across the European Union, and particularly so because of the somewhat contested nature what is instant notification processes. As such the approach that should suggested here is to closely match the text in the Directive.

Incidents are to be reported to the CSIRT first, rather than shared with/directed at National Competent Authorities. Where relevant the CSIRT can share information with the Competent Authorities.

Essentially, we want to ensure that (a) the CSIRT has the best possible situational awareness on events in the State, so all incident reports need to land there first and will be triaged as appropriate, including telling multiple NCAs if required. Also, (b) in order to ensure that national security related incidents don't make their way into the NIS system (re Article 2(6) of the Directive).

All public bodies should have a positive obligation to report significant cyber security incidents. In the interests of clarity and to reduce the burden on public bodies, it is proposed to use the definition and thresholds for significant incidents as provided for in the NIS 2 Directive.

The Department of Environment, Climate and Communications has also engaged with all Government Departments and a number of agencies on this issue. As a result of that

engagement the following are proposed for inclusion in the General Scheme as a public body obliged to report significant cyber security issues to the CSIRT in the NCSC:

- a local authority within the meaning of the Local Government Act 2001;
- a university within the meaning of the Universities Act 1997;
- any other person, body or organisation established—
    - by or under an enactment (other than the Companies Acts) or charter,
    - by any Scheme administered by a Minister of the Government, or
    - under the Companies Acts in pursuance of powers conferred by or under another enactment, and financed wholly or partly by means of money provided, or loans made or guaranteed, by a Minister of the Government or the issue of shares held by or on behalf of a Minister of the Government,
    - a company (within the meaning of the Companies Acts) a majority of the shares in which are held by or on behalf of a Minister of the Government,
    - any other person, body, organisation or group financed wholly or partly out of moneys provided by the Oireachtas that stands prescribed for the time being (being a person, body, organisation or group that, in the opinion of the Minister, following consultation with the Commission, ought, in the public interest and having regard to the provisions and spirit of this Act, to be prescribed);

Head 16- Coordinated Vulnerability Disclosure

(1) The NCSC, as CSIRT is designated as coordinator for the purposes of coordinated vulnerability disclosure, acting as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party.

(2) The tasks of the CSIRT in this regard shall include:
   a. identifying and contacting the entities concerned;
   b. assisting the natural or legal persons reporting a vulnerability; and
   c. negotiating disclosure timelines and managing vulnerabilities that affect multiple entities,
   d. ensuring that natural or legal persons are able to report, anonymously where they so request, a vulnerability;
   e. ensuring that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability.

(3) Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.

(4) The Minister may make regulations prescribing requirements to be imposed to implement this section.

Explanatory Note:

This Head relates to the transposition of Article 12 of the NIS2 Directive which gives effect to European coordinated vulnerability disclosure mechanism.

Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying such vulnerabilities is an important factor in reducing risk. Entities that develop or administer network and information systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and disclosed by third parties, the manufacturer or provider of ICT products or ICT services should also put in place the necessary procedures to receive vulnerability information from third parties. In that regard, international standards ISO/IEC 30111 and ISO/IEC 29147 provide guidance on vulnerability handling and vulnerability disclosure. Strengthening the coordination between reporting natural and legal persons and manufacturers or providers of ICT products or ICT services is particularly important for the purpose of facilitating the voluntary framework of vulnerability disclosure.

It is a requirement under the NIS2 Directive that Member States designate a CSIRT as a coordinator, acting as a trusted intermediary between the reporting of natural or legal persons and the manufacturers or providers of ICT products or ICT services, which are likely to be affected by the vulnerability, where necessary. The tasks of the CSIRT designated as coordinator should include identifying and contacting the entities concerned, assisting the natural or legal persons reporting a vulnerability, negotiating disclosure timelines and managing vulnerabilities that affect multiple entities (multi-party coordinated vulnerability disclosure). Where the reported vulnerability could have significant impact on entities in more than one Member State, the CSIRTs designated as coordinators should cooperate within the CSIRTs network, where appropriate.

Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to the manufacturer or provider of the potentially vulnerable ICT products or ICT services in a manner allowing it to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also include coordination between the reporting natural or legal person and the manufacturer or provider of the potentially vulnerable ICT products or ICT services as regards the timing of remediation and publication of vulnerabilities.

.

Head 17- Designation of Competent Authorities

(1) The Minister for the purposes of this Act, designates the following competent authorities in the State on the security of network and information systems in respect of carrying out activities under [Head 36 and 37 of this Act]:

a. Commission for the Regulation of Utilities (CRU) for the following sectors:
   i. Energy
   ii. Drinking Water
   iii. Waste Water

b. Commission for Communications Regulation (ComReg) for the following sectors:
   i. Digital Infrastructure
   ii. ICT Service Management
   iii. Space
   iv. Digital Providers

c. Central Bank of Ireland (CBI) for the following sectors:
   i. Banking
   ii. Financial Market

d. Irish Aviation Authority (IAA) for the following sectors:
   i. Transport - Aviation

e. Commission for Rail Regulation (CRR) for the following sector:
   i. Transport – Rail

f. The Minister for Transport for the following sector:
   i. Transport – Maritime

g. National Transport Authority (NTA) for the following sector:
   i. Transport – Road

h. An Agency or Agencies under the remit of the Minister for Health for the following sector:
   i. Health

i. The NCSC for all other sectors set out in Schedule I and II.

(2) The Minister may make Regulations providing for the designation or the discharge of duties of a competent authority in the State for the security of network and information systems in accordance with section (1). The Minister shall consult with such persons as the Minster considers appropriate for the purposes of this section. These persons may include:

a. a Minister of the Government;
b. bodies under the aegis of a Minister of Government;
c. designated competent authorities as per section (1);
d. the NCSC.

Explanatory Note:

The Head transposes the requirement regarding the designation of competent authorities under Article 8 of the NIS2 Directive. The designation of the above competent authorities was approved by Government in December 2023.

Other provisions regarding supervision and enforcement etc are set out in standalone Heads.

The Minister also has the ability via secondary legislation to designate additional competent authorities as required in consultation with the relevant persons the Minister considers appropriate. These persons will include Government Ministers, bodies under the aegis of Government Ministers, the designated competent authorities and the NCSC as lead competent authority for this Act.

The Minister also has the ability via secondary legislation to discharge a competent authority. This is only foreseen to arise in cases where legal certainty is required, eg if one of the bodies changes its name.

Head 18- Role of Lead Competent Authority

(1) The NCSC will act as lead competent authority for the purposes of this Act. Its duties shall include:

a. Acting as a central coordinator providing advice, guidance and support including development of regulatory framework and tools.
b. Acting as the central authority for engagement with European Commission, EU bodies and agencies, and other Member States.
c. Delivering a programme of support for Competent Authorities to support their capacity development, in particular staff recruitment, training and retention.

Explanatory Note:

The Head provides for the NCSC to act as the lead competent authority in the State for the implementation of NIS2. This is in recognition of the existing expertise built up in the NCSC in its role as a competent authority under the NIS Directive, which was transposed into Irish law via S.I. 360 of 2018.

The NCSC, acting as a central co-ordinating will provide guidance and support including the development of a regulatory framework and tools to assist the other competent authorities in carrying out their role under this Act.

This provision also provides clarity for the other designated competent authorities regarding the specific roles the NCSC will take on that do not have to.

This role is not provided for in the Directive, it was taken as a policy decision after engagement with the other competent authorities in agreement with the NCSC.

Head 19- Funding mechanism for Competent Authorities for their functions under this Act by way of levy.

(1) For the purpose of funding —

A competent authority which has an existing provision in statute to make an order imposing a levy on the entities it is designated to regulate, may make an order imposing a levy on the entities it is designated as competent authority for under Head 17 this Act for the purpose of meeting expenses properly incurred by the competent authority in the discharge of its functions of under this Act.

(2) "The Communications Regulation Act 2002 is amended—
in section 30—

(i) by inserting after subsection (2) the following:
"(2A) For the purpose of meeting expenses properly incurred by the Commission in the discharge of its function in relation to the Network and information Systems Directive (Directive (EU) 2022/2555), the Commission may make an order imposing a levy on [Digital Infrastructure providers, ICT Service Management (business to business) providers, Space and Digital Providers].
(ii) in subsection (3) by inserting "or the Network and information Systems Directive (Directive (EU) 2022/2555)
(iii) by substituting for subsection (11) the following:

"(11) The Commission shall not impose a levy on providers of—
(a) electronic communications for the purpose of meeting expenses properly incurred by the Commission in the discharge of its functions in respect of postal services or premium rate services or the Network and information Systems Directive (Directive (EU) 2022/2555),
(b) postal services for the purpose of meeting expenses properly incurred by the Commission in the discharge of its functions in respect of electronic communications services or premium rate services or the Network and information Systems Directive (Directive (EU) 2022/2555), or
(c) premium rate services for the purposes of meeting expenses properly incurred by the Commission in the discharge of its functions in respect of postal services or electronic communications services or the Network and information Systems Directive (Directive (EU) 2022/2555) or
(d) the Network and information Systems Directive (Directive (EU) 2022/2555) for the purposes of meeting expenses properly incurred by the Commission in the discharge of its functions in respect of postal services or electronic communications services or premium rate services."

Explanatory Note:

This Head amends the Communications Regulation Act 2002 to allow ComReg to extend its levy funding to its function under the Directive.

Ensuring adequate resources to meet the objectives of this Directive and to enable the competent authorities and the CSIRTs to carry out the tasks laid down herein is essential. A financing mechanism to cover necessary expenditure in relation to the conduct of tasks of public entities responsible for cybersecurity in the State under this Act. Taking into consideration a number of the designated competent authorities are Levy funded in full or part for the execution of their functions

under their respective legislation. It is intended that they are allowed to extend their current levy model to their activities under this Act.

This [Act] will act as the legislative vehicle for the relevant Departments and agencies to amend their own Primary legislation, subject to standard approval procedures, to extend their levy funding to their activities under the Directive.

Head 20 – Scope of this Act

(1) This Act applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article.
(2) Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of this Directive.
(3) This Act applies without prejudice to the State's responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.
(4) Regardless of their size, this Directive applies to entities identified as critical entities under [Directive (EU) 2022/2557].
(5) Regardless of their size, this Act also applies to entities providing domain name registration services.
(6) This [Act] does not apply to entities which the State has exempted from the scope of [Regulation (EU) 2022/2554] in accordance with [Article 2(4) of that Regulation]
(7) This Act applies without prejudice to:
    a. The Data Protection Act 2018
    b. S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011.
    c. S.I. No. 309/2015 - European Union (Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography) Regulations 2015.
    d. The Criminal Justice (Offences relating to Information Systems) Act of 2017
    e. Directive (EU) 2022/2557
(8) [Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities in accordance with this Directive only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of entities concerned.]

Explanatory Note:

This Head provides for the general application or scope of this Act by transposing the specific provisions in Article 2 of the Directive. It also sets out a number of exemptions.

- This Act does not apply to entities which the State has exempted from the scope of [Regulation (EU) 2022/2554] in accordance with [Article 2(4) of that Regulation]. The DORA Regulation comes into force in January 2025. The Department of Finance is responsible for giving full effect to this Regulation in the State.
- This Act applies without prejudice to
    - Regulation (EU) 2016/679 given full effect in Irish law by the Data Protection Act 2018
    - Directive 2002/58/EC was transposed into Irish law by S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011.

- Directives 2011/93/EU (27) was transposed into Irish law by S.I. No. 309/2015 - European Union (Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography) Regulations 2015.
- Directive 2013/40/EU (28) was transposed into Irish law by the Criminal Justice (Offences relating to Information Systems) Act of 2017
- Directive (EU) 2022/2557. The Department of Defence are currently transposing this Directive into Irish law via S.I.

Head 21- Essential and Important Entities

(1) For the purposes of this Act the following entities shall be considered to be essential entities:
   a. entities of a type referred to in Schedule I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC;
   b. qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;
   c. providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC;
   d. public administration entities as set out in Head 23
   e. any other entities of a type referred to in Schedule I or II that are designated by the Minister as essential entities pursuant to Head 22;
   f. an entity identified as a critical entity under Directive (EU) 2022/2557
   g. an entity designated as operators of essential services under Part 4 of S.I. No. 360 of 2018, operators of essential services.

(2) For the purposes of this Act, entities of a type referred to in Schedule I or II which do not qualify as essential entities pursuant to section 1 shall be considered to be important entities. This includes entities designated by Minister as important entities pursuant to Head 22.

(3) By 17 April 2025, the NCSC shall establish a list of essential and important entities as well as entities providing domain name registration services, which shall be reviewed and, where appropriate, updated, on a regular basis and at least every two years thereafter.

(4) For the purpose of establishing the list referred to in section (3), the Minister shall require the entities referred to in that section to submit at least the following information to the relevant competent authorities:
   a. the name of the entity;
   b. the address and up-to-date contact details, including email addresses, IP ranges and telephone numbers;
   c. where applicable, the relevant sector and subsector referred to in Schedule I or II; and
   d. where applicable, a list of the Member States where they provide services falling within the scope of this Directive.

(5) In addition, in order to assist in the identification of systemic risks, the following information shall be submitted to the NCSC, on request, if it underpins the Essential or Important Services described in Annex I and II provided by the entity:
   a. Names of the following service providers;
   b. cloud computing service provider;
   c. data centre service provider;
   d. public electronic communications network provider;
   e. electronic communications service;
   f. managed service provider;
   g. managed security service provider;
   h. technology vendor

(6) The entities referred to in section 2 shall notify any changes to the details submitted pursuant to the first subsection of this section without delay, and, in any event, within two weeks of the date of the change.

(7) By 17 April 2025 and every two years thereafter, the NCSC shall notify:

(8) the Commission and the Cooperation Group of the number of essential and important entities listed pursuant to section 3 for each sector and subsector referred to in Schedule I or II; and

(9) the Commission of relevant information about the number of essential and important entities identified pursuant to Head 22(2)(a)-(d), the sector and subsector referred to in Schedule I or II to which they belong, the type of service that they provide, and the provision, from among those laid down in Head 22(2)(a)-(d), pursuant to which they were identified.

(10) Until 17 April 2025 and upon request of the Commission, The NCSC may notify the Commission of the names of the essential and important entities referred to in section 6(b).

(11) Entities falling within the scope of this Act shall be considered to fall under the jurisdiction of the Member State in which they are established, except in the case of:

a. providers of public electronic communications networks or providers of publicly available electronic communications services, which shall be considered to fall under the jurisdiction of the Member State in which they provide their services;

b. DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2;

c. public administration entities, which shall be considered to fall under the jurisdiction of the State which established them.

(12) For the purposes of this Act, an entity as referred to in section (8)(b) shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union.

(13) If an entity as referred to in section (8)(b)), is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. In the absence of a representative in the Union designated under this section, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Act.

(14) The designation of a representative by an entity as referred to in section (8)(b) shall be without prejudice to legal actions, which could be initiated against the entity itself.

(15) A relevant designated competent authority that receives a request for mutual assistance in relation to an entity as referred to in section (8)(b) may, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has a network and information system on their territory.

Explanatory Note:
This Head transposes Article 3 and Article 26 of the NIS 2 Directive.

In order to ensure a clear overview of the entities falling within the scope of the NIS 2 Directive, the NCSC needs to establish a list of essential and important entities as well as entities providing domain name registration services. For that purpose, the NCSC requires entities to submit at least the following information to the competent authorities, namely, the name, address and up-to-date contact details, including the email addresses, IP ranges and telephone numbers of the entity, and, where applicable, the relevant sector and subsector referred to in the annexes, as well as, where applicable, a list of the Member States where they provide services falling within the scope of this Directive.

Article 26 relates to the jurisdiction and territoriality of an entity and sets out the provisions regarding the 'main establishment' rule.

The NCSC should be able to establish national mechanisms for entities to register themselves. The NCSC can decide on the appropriate mechanisms that allow for the identification of entities falling within the scope of this Directive.

The NCSC must submit to the Commission at least the number of essential and important entities for each sector and subsector referred to in the annexes, as well as relevant information about the number of identified entities and the provision, from among those laid down in the NIS 2 Directive, on the basis of which they were identified, and the type of service that they provide.

On request from the NCSC, Entities must submit the following additional information, if it underpins the Essential or Important Services described in Annex I and II provided by the entity.

	Definition
Cloud computing service provider	Article 6 (30)
Data centre service provider	Article 6 (31)
Public electronic communications network provider	Article 6 (36)
Electronic communications service	Article 6 (37)
Managed service provider'	Article 6 (39)
Managed security service provider	Article 6 (40)
Technology vendors	Hardware and Software

Head 22 – Designation of Other Entities under Schedule I or II

(1) Regardless of their size, this Act shall apply to any entity, under Schedule I or II where:
   a. the person provides public electronic communications networks or of publicly available electronic communications services;
   b. the person is a trust service provider;
   c. the person provides top-level domain name registries and domain name system service providers;

(2) The Minister may make Regulations providing for the designation of a person as an essential or important entity in a sector where that he/she is satisfied that—
   a. the person is the sole provider in the State of a service which is essential for the maintenance of critical societal or economic activities;
   b. disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;
   c. disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;
   d. the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;

(3) The Minister shall consult with such persons as the Minster considers appropriate for the purposes of this section. These persons may include:
   a. a designated competent authority as per Head 17;
   b. the NCSC.

Explanatory Note:
This Head transposes the specific provisions in Article 2(2)(a)-(e) of the NIS2 Directive. The scope here is very broad, so it is proposed that the Minister may make Regulations designating a person as an Essential or Important entity under this Head, where the criteria is very broad.

Head 23- Public Administration

(1) In this Act, "an essential public administration entity" means—
   a. a Minister of the Government;
   b. Central Statistics Office;
   c. Office of the Comptroller and Auditor General;
   d. Office of the Revenue Commissioners;
   e. The Office of Public Works;
   f. The National Shared Services Office

(2) The entities listed in section (1) shall be considered essential entities as per Head 21.

(3) Any other entity that means the definition of a public administration body shall be considered as an important entity as per Head 21.

(4) The Minister may, on foot of an assessment of the risk to the State of their ICT systems being affected by a cyber security incident designate a body that would not otherwise be included in the definition of "public administration entity" in section (1) and with the consent of the Minister of the Government in whom functions in relation to that body are vested, by order designate that body as a public administration entity where—

(5) the Minister is satisfied the body:
   a. is established for the purpose of meeting needs in the general interest to citizens and does not have an industrial or commercial character;
   b. has legal personality or is entitled by law to act on behalf of another entity with legal personality;
   c. is financed, for the most part, by the State, regional authorities or by other bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities or by other bodies governed by public law;
   d. has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.

(6) The assessment of risk as set out in section (3) will be carried out by an inter-agency task force.

(7) The Minister may prescribe the procedure for –
   a. The assessment of risk assessment and the establishment of the inter-agency task force set out under section (4).

Explanatory Note:

This Head sets out the provisions regarding how Essential public administration entities are dealt with in this Act.

The Public Administration sector is listed among the categories of Essential Entities in Schedule 1 of this Act. These Essential Entities will be required to implement cyber security risk management measures and processes, to report significant cyber security incidents, and will be subject to external supervision with penalties for non-compliance.

The Directive explicitly states that public bodies of central government as defined in Article 6(35) of the Directive fall within scope regardless of their size. This is to be defined in national legislation. The Directive also states that regional bodies whose criticality is identified through an appropriate risk assessment will be within the scope of the Directive. Entities involved in national security, defence, or law enforcement fall outside the scope.

Public administration entities at local level and educational institutions are outside the scope of the Directive, but Member States may include them. For educational institutions, attention should be paid to those carrying out critical research activities. Public bodies carrying out functions that fall within other sectors set out in the Directive, e.g. healthcare, will fall will within scope of these sectors and be dealt with separately.

The Minister for the Environment, Climate and Communications will be able to designate public bodies as essential entities by means of Ministerial regulations on completion of a risk assessment by an inter-agency task force.

The establishment of the inter-agency task force and further detail regarding the risk assessment procedure will be prescribed by the Minister in due course.

It should be noted, if an entity meets the definition of a public administration entity under this [Act] then it will be an important entity for the purposes of this [Act]

Head 24- National Cyber Security Strategy

(1) The Minister shall prepare a national strategy on the security of network and information systems (the "National Cyber Security strategy").

(2) The National Cyber Security strategy shall set out:

a. objectives and priorities of the cybersecurity strategy covering in particular the sectors referred to in Schedule I and II;

b. a governance framework to achieve the objectives and priorities referred to in point (a) of this section, including the policies referred to in section 2;

c. a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs under this Act, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts;

d. a mechanism to identify relevant assets and an assessment of the risks in the State;

e. an identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors;

f. a list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy;

g. a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate;

h. a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens.

(3) As part of the national Cyber Security strategy, the State shall in particular adopt policies:

a. addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;

b. on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;

c. managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Head 16;

d. related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables;

e. promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;

f. promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities;

g. supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure;

h. including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with GDPR and the Data Protection Act 2018;

i. strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs;
j. promoting active cyber protection.

(4) The Minister may publish in such form and in such manner as he or she considers appropriate a draft of the proposed national strategy.
(5) Where a draft of the proposed national strategy is published in accordance with section (4), a person may make written submissions or representations to the Minister in relation to the draft within a period of thirty working days from the date on which that draft is published.
(6) The Minister shall consider any submissions or representations made to him or her under section (6).
(7) The Minister shall cause a copy of the national strategy to be laid before each House of the Oireachtas and, not more than 5 working days after the national strategy is so laid before the Houses of the Oireachtas, the Minister shall cause it to be published in such form and in such manner as the Minister considers appropriate.
(8) The Minister may review the national strategy at any time and, in any event, shall review it not later than 4 years on the basis of key performance indicators and, where necessary, update it.
(9) Where, after carrying out a review referred to in paragraph (8), the Minister decides to revise the national strategy, paragraphs (3) to (5) and (7) shall apply, with necessary modification, in respect of any such revision.
(10) The Minister may, in preparing the national strategy or any revisions thereto, request the assistance of ENISA.

Explanatory Note:

This Head directly transposes Article 7 of Directive: National Cyber Security Strategy, substituting Member State for the Minister.

The current National Cyber Security Strategy 2019-2024 is an obligation set out in SI 360 of 2018. The requirements of the National Cyber Security Strategy as set out in Article 7 of the Directive greatly expand on the requirements of the current strategy. The Department will use these provisions as the basis for the establishment of the National Cyber Security Strategy 2025 – 2030.

The provisions regarding the review and publication of the strategy mirror those in Part 3 of S.I. 360 of 2018.

Head 25- The Application of Sector-specific Union legal acts

(1) Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Act, the relevant provisions of this Act, including the provisions on supervision and enforcement laid down in Part 8, shall not apply to such entities. Where sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Act, the relevant provisions of this Act shall continue to apply to the entities not covered by those sector-specific Union legal acts.

(2) The requirements referred to in section (1) of this Head shall be considered to be equivalent in effect to the obligations laid down in this Act where:

a. cybersecurity risk-management measures are at least equivalent in effect to those laid down in [Head 29(1) and (2)] or

b. the sector-specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the CSIRTs, the competent authorities or the single points of contact under this Directive and where requirements to notify significant incidents are at least equivalent in effect to those laid down in Head 15(1) to (6) of this Act.

Explanatory Note:

This Head transposes Article 4 - Sector-specific Union legal acts. This provision is an enabling one as there are a number of pieces of EU legislation that contains cyber security measures.

The Guidance provided from ENISA states that Member States should not apply the provisions of Directive (EU) 2022/2555 (NIS2 Directive) on cybersecurity risk-management and reporting obligations, and supervision and enforcement, to financial entities covered by Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA).

DORA comes into effect in January 2025. The Department of Finance will be giving full effect in the State to this Regulation.

Therefore the Central Bank as a Competent Authority under the Directive, will not have to

- Maintain a register of the Banking/FMI entities under the Directive.
- Supervise Banking and Financial Management entities under the Risk Management Provisions

Part 4- Co-Operation at European Union and International Level

Head 26 – Cooperation at National Level

(1) The competent authorities designated in [Head 17] and the NCSC, in its roles as the CSIRT and Single Point of Contact under this Act shall cooperate with each other with regard to the fulfilment of their obligations laid down in this [Act].

(2) Essential and Important entities shall notify, without undue delay, the CSIRT in accordance with Head 15 of any incident that has a significant impact on the provision of their service.

(3) In addition to the notification obligation provided for in [Head 15], notifications can be submitted to the NCSC, on a voluntary basis, by:
   a. Essential and Important entities with regard to incidents, cyber threats and near misses;
   b. Entities other than those referred to in (4), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.

(4) The CSIRT designated under [Head 12] shall inform the single point of contact designated under [Head 13] of notifications of incidents, cyber threats and near misses submitted pursuant to this [Act].

(5) The NCSC shall ensure to the extent possible that single points of contact and the CSIRTs cooperate appropriately as set out in [Head 11] and also:
   a. The State Authority under Air Navigation and Transport Act 2022;
   b. The State Authority under Electronic Commerce Act 2000;
   c. Competent authorities under Regulation (EU) 2022/2554;
   d. National regulatory authority under the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023
   e. Competent authorities under Directive (EU) 2022/2557

(6) The NCSC shall simplify the reporting through technical means for notifications referred to in [Heads 15 and Head 33].

Explanatory Note:

This Head relates to the transposition of Article 13 of the NIS2 Directive which sets out cooperation between the various entities designated under this Bill. This provision in the main points back to other provisions in the [Act] and also out to other State Legislation as follow:

(13) Air Navigation and Transport Act 2022 gives full effect to Regulation (EC) No 300/2008 and (EU) 2018/1139. A Minister of the Government, the Commissioners of Public Works Ireland or an agent of the Minister is the State authority for this legislation.
Electronic Commerce Act 2000 gives full effect to Regulation No 910/2014. The Minister for the Environment, Climate and Communications is responsible for the supervision of this legislation.

(14) Regulation (EU) 2022/2554 (DORA) will be give full effect in the State by legislation currently being drafted by the Department of Finance. The Central Bank of Ireland will be at least one of the Competent Authorities under this legislation.

(15) Directive (EU) 2018/1972 was transposed into Irish law by the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023. ComReg is the National Regulatory Authority under this Act.

(16) Directive (EU) 2022/2557 (CER) is currently being transposed into Irish Law by the Department of Defence. It is expected many of the same Competent Authorities for this Directive will be the same as the CER Directive.

Many of the bodies who fulfil the role of Competent authority, States Authority and National Regulatory Authorities under the legislation listed and under this legislation are the same meaning they are fulfilling multiply roles. Therefore, cooperation at National level should be more achievable via forums such as the National Competent Authority Forum which is being led by the NCSC for the Directive.

Head 27- Cooperation Group

(1) The NCSC shall ensure effective, efficient, and secure cooperation of their representatives in the Cooperation Group.

Explanatory Note:
This Head relates to the transposition of Article 14 (5) of the NIS2 Directive which sets out that the NCSC will ensure effective, efficient, and secure cooperation of their representatives in the Cooperation Group. The Cooperation Group was created under Directive (EU) 2016/1148 of The European Parliament and Of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Part 5 - Cyber Security Risk Management Measures and Reporting Obligations

Head 28- Governance

(1) The management board of essential and important entities shall:
   a. approve the cyber security risk-management measures taken by those entities in order to comply with Head 29;
   b. oversee implementation of Head 29 by those entities; and
   c. be held liable for infringements as set out under Part 8 of this [Act] by the entities of that Head.
   d. The relevant designated competent authority shall monitor the measures set out in section (1).

(2) The relevant designated competent, when exercising its enforcement powers in relation to section (2), have the powers pursuant to Part 8.

(3) The management bord of essential and important entities are required to follow cyber security risk-management training and shall encourage their employees to take relevant cyber security training on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Explanatory Note:

This Head transposed the relevant provisions of Article 20 of the NIS2 Directive. In order to ensure a high level of responsibility for the cybersecurity risk-management measures and reporting obligations at the level of the essential and important entities, the management bodies of the essential and important entities should approve the cybersecurity risk-management measures and oversee their implementation.

The application of this section shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.

Members of management bodies of essential and important entities are required to follow training and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Under this Act, organisational management and executives can be found personally liable if gross negligence is found following a cybersecurity incident. Management can be mandated to publicly disclose instances of, and the identity of the legal person(s) responsible for, non-compliance.

Head 29- Cyber Security Risk-Management Measures

(1) Essential and important entities shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

(2) Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in section (1) shall ensure a level of security of network and information systems appropriate to the risks posed.

(3) When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

(4) The measures referred to in section (1) shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

(5) When considering which measures referred to in section 4(d) are appropriate, entities shall take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. When considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out by the co-operation group in accordance with Article 22(1) of the Directive.

(6) A relevant designated competent authority that is made aware that an entity does not comply with the measures provided for in section (4) takes, without undue delay, all necessary, appropriate and proportionate corrective measures as per Part 8 of this Act.

(7) The Minister, having consulted with the all the relevant designated competent authorities, may make Regulations in relation to the types of cyber security risk management measures to be taken by Essential and Important Entities in accordance with section (4) of this Head.

Explanatory Note:

This Head transposes Article 21 of the NIS 2 Directive on cybersecurity risk management measures. It is proposed drop one single unitary section on risk management measures because of the way in which NIS2 does not differentiate between different classes of entity at this stage.

By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in section 2 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

Articles 32 and 33 set out very different sets of supervisory and enforcement requirements, but this article essentially establishes the nature of the measures required.

This Head also allows for the Minister to make Regulations in relation to the types of cyber security risk management measures to be taken by Essential and Important Entities.

There is also a reference made to coordinated security risk assessments of critical supply chains as per Article 22(1) of the Directive. That Article was not transposed as it a role for the Co-operation group.

Head 30- Use of Cyber Security Certification Schemes

(1) In order to demonstrate compliance with particular requirements of Cyber Security risk-management measures per Head 29-

(2) an essential or important entities may be required to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under a European cyber security certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881; or

(3) an essential or important entities may be advised to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under a national cyber security certification scheme.

Explanatory Note:

This Head transposes the relevant provisions of Article 24 of the NIS 2 Directive to require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cyber security certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881.

While the Directive allows for mandatory certification to demonstrate compliance, there is no plan to mandate this type of certification in the short to medium term within the State, and that provision within the Directive text is there more so to allow the Commission to do this via a European cybersecurity certification scheme at some point in the future.

This Head also provides that in the future essential and important entities could be advised to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under a National cyber security certification scheme. The NCSC will seek sanction from the Irish National Accreditation Board (INAB) for a voluntary national cybersecurity certification scheme, where independent 3rd party accredited certification conducted by Conformity Assessment Bodies to the requirements of the national scheme, will provide Important and Essential NIS2 entities who seek certification under the relevant assurance level of the national scheme, to demonstrate their compliance with the relevant NIS2 security measures.

The scheme is currently under development, and it is proposed that the finalised scheme will contain at least one assurance level that will comprise of controls and requirements based on the NIS2 security measures. This will allow Important and Essential entities to be able to display to National Competent Authorities that they have implemented the cybersecurity policies and controls that demonstrate compliance with the legally required NIS2 security measures.

Regulation (EU) 2019/881 has not been given full effect in the State and there are currently no National cyber security certification schemes in place. However, this provision is an enabling one to allow for the use of these schemes if required when they are available.

Part 6- Registration

Head 31- Registry of entities

(1) DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, shall submit the following information to the NCSC by 17 January 2025:
   a. the name of the entity;
   b. the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable;
   c. the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Head 21(10);
   d. up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative designated pursuant to [Head X (x)];
   e. the Member States where the entity provides services; and
   f. the entity's IP ranges.

(2) Entities referred to in section (1) shall notify the competent authority about any changes to the information they submitted under section (1) without delay and in any event within three months of the date of the change.

(3) Upon receipt of the information referred to in sections (1) and (3), except for that referred to in section 1, point (f), the single point of contact of the State shall, without undue delay, forward it to ENISA.

(4) Where applicable, the information referred to in sections (1) and (3) shall be submitted through the national mechanism referred to in [Head 32].

Explanatory Note:

This Head transposes Article 27 of the NIS 2 Directive. In order to ensure a clear overview of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, which provide services across the Union that fall within the scope of the NIS2 Directive, ENISA should create and maintain a registry of such entities, based on the information received by Member States, where applicable through national mechanisms established for entities to register themselves.

The single points of contact should forward to ENISA the information and any changes thereto. With a view to ensuring the accuracy and completeness of the information that is to be included in that registry, Member States can submit to ENISA the information available in any national registries on those entities.

ENISA and the Member States should take measures to facilitate the interoperability of such registries, while ensuring protection of confidential or classified information. ENISA should establish appropriate information classification and management protocols to ensure the security and confidentiality of disclosed information and restrict the access, storage, and transmission of such information to intended users.

Head 32- Database of domain name registration data

(1) TLD name registries and entities providing domain name registration services shall collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with GDPR Regulation and the Data Protection Act 2018 as regards data which are personal data.

(2) For the purposes of section 1, the database of domain name registration data shall contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include:
   a. the domain name;
   b. the date of registration;
   c. the registrant's name, contact email address and telephone number;
   d. the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.

(3) The TLD name registries and the entities providing domain name registration services shall make publicly available policies and procedures, including verification procedures, in place to ensure that the databases referred to in section (1) include accurate and complete information.

(4) The TLD name registries and the entities providing domain name registration services shall make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.

(5) The TLD name registries and the entities providing domain name registration services shall:

(4) provide access to the [relevant competent authority designated under Head 17] to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with [Union data protection law];

(5) reply without undue delay and in any event within 72 hours of receipt of any requests for access;

(6) make policies and procedures with regard to the disclosure of such data publicly available.

(6) Compliance with the obligations laid down in sections (1) – (5) shall not result in a duplication of collecting domain name registration data. To that end, the TLD name registries and entities providing domain name registration services shall cooperate with each other. in order to avoid the duplication of the collection of domain name registration data

Explanatory Note:
This Head transposes Article 28 of the NIS 2 Directive. Maintaining accurate and complete databases of domain name registration data (WHOIS data) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity across the Union. For that specific purpose, TLD name registries and entities providing domain name registration services should be required to process certain data necessary to achieve that purpose. Such processing should constitute a legal obligation within the meaning of Article 6(1), point (c), of Regulation (EU) 2016/679. That obligation is without prejudice to the possibility to collect domain name registration data for other purposes, for example on the basis of contractual arrangements or legal requirements established in other Union or national law. That obligation aims to achieve a complete and accurate set of registration data and should not result in collecting the same data multiple times. The TLD name registries and the entities providing domain name registration services should cooperate with each other in order to avoid the duplication of that task.

The availability and timely accessibility of domain name registration data to legitimate access seekers is essential for the prevention and combating of DNS abuse, and for the prevention and detection of and response to incidents. Legitimate access seekers are to be understood as any natural or legal person making a request pursuant to Union or national law. They can include authorities that are competent under this Directive and those that are competent under Union or national law for the prevention, investigation, detection or prosecution of criminal offences, and CERTs or CSIRTs. TLD name registries and entities providing domain name registration services should be required to enable lawful access to specific domain name registration data, which are necessary for the purposes of the access request, to legitimate access seekers in accordance with Union and national law. The request of legitimate access seekers should be accompanied by a statement of reasons permitting the assessment of the necessity of access to the data.
In order to ensure the availability of accurate and complete domain name registration data, TLD name registries and entities providing domain name registration services should collect and guarantee the integrity and availability of domain name registration data. In particular, TLD name registries and entities providing domain name registration services should establish policies and procedures to collect and maintain accurate and complete domain name registration data, as well as to prevent and correct inaccurate registration data, in accordance with Union data protection law. Those policies and procedures should take into account, to the extent possible, the standards developed by the multi-stakeholder governance structures at international level. The TLD name registries and the entities providing domain name registration services should adopt and implement proportionate procedures to verify domain name registration data. Those procedures should reflect the best practices used within the industry and, to the extent possible, the progress made in the field of electronic identification. Examples of verification procedures may include ex ante controls carried out at the time of the registration and ex post controls carried out after the registration. The TLD name registries and the entities providing domain name registration services should, in particular, verify at least one means of contact of the registrant.

TLD name registries and entities providing domain name registration services should be required to make publicly available domain name registration data that falls outside the scope of Union data protection law, such as data that concern legal persons, in line with the preamble of [Act] (EU) 2016/679. For legal persons, the TLD name registries and the entities providing domain name registration services should make publicly available at least the name of the registrant and the contact telephone number. The contact email address should also be published, provided that it does not contain any personal data, such as in the case of email aliases or functional accounts. TLD name registries and entities providing domain name registration services should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should require TLD name registries and entities providing domain name registration services to respond without undue delay to requests for the disclosure of domain name registration data from legitimate access seekers. TLD name registries and entities providing domain name registration services should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. Those policies and procedures should take into account, to the extent possible, any guidance and the standards developed by the multi-stakeholder governance structures at international level. The access procedure could include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission can, without prejudice to the competencies of the European Data Protection Board, provide guidelines with regard to such procedures, which take into account, to the extent possible, the standards developed by the multi-stakeholder governance structures at international level. Member States should ensure that all types of access to personal and non-personal domain name registration data are free of charge.

Part 7- Information Sharing

Head 33- Cyber Security information-sharing arrangements

(1) On a voluntary basis, entities falling within the scope of this [Act] and, where relevant, other entities not falling within the scope of this [Act] should exchange relevant cyber security information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

a. aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

b. enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.

(2) The NCSC will ensure the exchange of information shall take place within communities of essential and important entities, including within the Sectors set out in Schedule I and II, and where relevant, their suppliers or service providers. Such exchange shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared.

(3) The NCSC shall:

a. facilitate the establishment of cybersecurity information-sharing arrangements referred to in section (2). Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements. In laying down the details of the involvement of public authorities in such arrangements.

b. offer assistance for the application of such arrangements by developing and sharing policies referred to in Head 24(3)(h) for this purpose.

(4) The Essential and Important entities shall notify their designated competent authority of their participation in the cybersecurity information-sharing arrangements referred to in section (2), upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.

Explanatory Note:

This Head transposes Article 29 of the NIS 2 Directive. Entities falling both in scope and not of this Act should have the ability to share cyber security information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks.

This information sharing is done on a voluntary basis, with the support of the NCSC, as the National CSIRT and Lead Competent Authority. As such the intention is to allow flexibility in how this is done in practicality.

The NCSC has established and leads a forum for the National Competent Authorities. It also facilitates information sharing with Sectoral bodies. Due to the sensitively of that information, we are not prescribing in the [Act] how that is being done, but here is an obligation under Head 24(3)(h) for the NCSC to adopt policies including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with GDPR and the Data Protection Act 2018.

Head 34- Voluntary notification of relevant information

(1) In addition to the notification obligation provided for in [Head 15], notifications can be submitted to the NCSC, on a voluntary basis, by:
   a. essential and important entities with regard to incidents, cyber threats and near misses;
   b. entities other than those referred to in (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.

(2) The NCSC, as CSIRT shall process the notifications referred to in section 1 of this Head in accordance with the procedure laid down in [Head 15]. Member States may prioritise the processing of mandatory notifications over voluntary notifications.

(3) Where necessary, the competent authorities shall be provided with information about notifications received pursuant to this Article shall be sent to the NCSC, as CSIRT and single point of contact, while ensuring the confidentiality and appropriate protection of the information provided by the notifying entity.

(4) Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.

Explanatory Note:

This Head transposed Article 30 of the Directive - Voluntary notification of relevant information.

All entities in the State are encouraged to report to the CSIRT on incidents, cyber threats and near misses regardless of whether or not they fall into scope of this Act of not.

Entities under section (1)(b) include public bodies, who are not defined under this [Act] as a public body or an essential public administration entity.

Part 8- Supervision and Enforcement

Head 35 – Definitions

(1) In this Part—

"a place" includes any premises or other place or any train, vessel, vehicle or aircraft.

'person in charge', in relation to a place, means—

the person under whose direction and control the activities at that place are being conducted, or

the person whom the authorised officer has reasonable grounds for believing is in control of that place;

'record' includes any memorandum, book, report, statement, register, plan, chart, map, drawing, specification, diagram, pictorial or graphic work or other document, any photograph, film or recording (whether of sound or images or both), any form in which data (including data that constitute personal data) are held, any form (including machine-readable form) or thing in which information is held or stored manually, mechanically or electronically, and anything that is a part or copy, in any form, of any of, or any combination of, the foregoing.

Explanatory Note

This Head is to allow for the definition of terms in this part of the Act. While there are a limited number of definitions contained here, this may expand during drafting and there are also provisions already made at Head 2 to define terms across the entire act.

Head 36- Supervisory and enforcement measures in relation to Essential Entities

1) For the purposes of the exercise by a designated National Competent Authority of its supervisory functions under this Act, or any regulations made under this Act, in relation to any Essential Entity, an authorised officer may—
   a) give a direction to the entity requiring it, at such time or times and place or places, and in such manner, as may be specified in the direction, to allow security audits of its processes and systems, to be conducted by an independent third party, or by the competent authority,

      and, or,

   b) give a direction to the entity requiring it, at such time or times and place or places, and in such manner, as may be specified in the direction to submit to any other ad-hoc security audit as deemed necessary by the authorised officer including where justified on the ground of a significant incident or an infringement of this Act or the Directive by the essential entity,

      and, or

   c) give a direction to the entity requiring it to give all assistance to the authorised officer or any other person nominated by the authorised officer as the Essential Entity is reasonably able to give in order to conduct a security scan of the entity's systems,

      and, or,

   d) give a direction to the entity requiring it, at such time and place, and in such manner, as may be specified in the direction, to produce such records as are specified in the direction that,

      i) appear necessary to the authorised officer to assess the cybersecurity risk-management measures adopted by the entity concerned,

         and, or,

      ii) appear necessary to the authorised officer to assess the implementation of cybersecurity policies,

         and, or,

      iii) appear necessary to the authorised officer to carry out their supervisory functions.

2) The authorised officer shall give a direction at section (1)(a) only where a risk assessment conducted by the National Competent Authority, or by the Essential Entity, has been conducted, or where any other information causes the authorised officer to consider that there are sufficient grounds of risk to give the direction.
3) Any direction given by an authorised officer at section (1)(a) or section (1)(b) shall require the Essential Entity, or any third party performing the audit, to provide any and all such information concerning the audit, as deemed necessary, to the authorised officer.

4) The costs of any security audit carried out by an independent body in compliance with section (1)(a) or (1)(b) shall be paid by the essential entity, except in duly substantiated cases where the competent authority decides otherwise.
5) When giving a direction under section 1 (d), the authorised officer shall state the purpose of the request and specify the information requested.

Explanatory Note

This Head transposes the enforcement piece of Article 32 of the Directive. In relation to Essential Entities it empowers authorised officers of Competent Authorities to issue directions to be subjected to security audits, hand over documents and records relating to the cybersecurity provisions within the Entity, conduct security scans and provides the basis on which they can be done.

Head 36A – Compliance Notices (Essential Entities)

1) An authorised officer who is of the opinion that an Essential Entity is committing or engaging in, an activity or practice, or is contravening or has contravened an enactment specified in the Act, may serve, personally or by post or by electronic means, a written notice on that Essential Entity (a "compliance notice").
2) A compliance notice shall be signed and dated by the authorised officer and shall—
   a) contain a statement of the alleged contravention, the opinion referred to in subsection (6) and the reasons for that opinion, and
   b) direct the entity to adopt any measures that, in the opinion of the authorised officer, are necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation,

      and, or,

   c) direct the entity to cease any conduct that infringes this Act and desist from repeating that conduct,

      and, or,

   d) direct the entity to ensure that their cybersecurity risk-management measures comply with Head 29 of the Act or to fulfil the reporting obligations laid down in Head 15 of this Act, in a specified manner and within a specified period of time,

      and, or,

   e) direct the entity to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat,

      and, or,

   f) direct the entity to implement the recommendations provided as a result of a security audit within a specified period of time,

      and, or,

   g) direct the entity to designate a monitoring officer with well-defined tasks for a specified period of time to oversee the compliance of the entity with Head 15 and Head 29 of this Act,

   h) and, or,

   i) direct the entity to make public aspects of infringements of this Act in a specified manner

   j) and contain a statement that the person may appeal the notice to the District Court within 14 days after service of the notice, including information specifying –

i) the form and manner of such an appeal, and
ii) the service address of the National Competent Authority for purposes of notifying the National Competent Authority under subsection (6),

and

k) contain a statement that, if an appeal is not made in accordance with this section and within the time specified in paragraph (j), then—

i) the notice will be treated as not disputed,

ii) the Essential Entity will be deemed to have accepted the notice and have agreed to comply with the compliance direction and requirements, and

iii) any failure or refusal to so comply is a contravention of this section and the entity will be liable to the penalties as set out in Head 36B.

3) A Competent Authority can publish warnings about infringements of this Act by the Essential Entity to whom it has issued a compliance notice.
4) Subject to subsection (b),
   a) a compliance notice shall be complied with within such period as may be specified in the notice which period shall not be less than 14 working days after the date of the notice.
   b) Upon the written application of the person on whom a notice is served, the period specified in the notice as the period within which that notice must be complied with may be extended by and at the discretion of the competent authority and, where the period is so extended, the compliance notice shall be complied within such extended time period.
5) An entity on whom a compliance notice has been served shall confirm in writing to the competent authority concerned that the compliance notice has been complied with as soon as practicable after so complying and in any case not later than 7 working days after the date specified in the notice by which it is to be complied with or, where the period of time has been extended under section (4), the date specified in accordance with the extension.
6) Where a person on whom a compliance notice has been served so confirms in writing under section (5) that the compliance notice has been complied with, the competent authority shall, on being so satisfied, not later than one month after the date of receipt of such confirmation, serve notice on the person concerned of compliance with the compliance notice.
7) The date specified under subsection (2)(b), (2)(d) and 2(f) shall not be earlier than the end of the period within which an appeal may be made under subsection (8).
8) If the Essential Entity on whom the compliance notice is served wishes to dispute the notice, the Entity may, no later than 14 days after the notice is served and in accordance with this section and in the form and manner specified in the notice, appeal the notice to a judge of the District Court in the district court district in which the notice was served.
9) An Entity who appeals under subsection (8) shall at the same time notify the designated National Competent Authority of the appeal and the grounds for the appeal and the National Competent Authority shall be entitled to appear, be heard and adduce evidence on the hearing of the appeal.
10) In determining an appeal under this section, the judge may confirm, vary or cancel the compliance notice, if satisfied that it is reasonable to do so.

11) If on appeal the compliance notice is not cancelled, the notice takes effect on the later of the following:
    a) the day after the day on which the notice is confirmed or varied on appeal;
    b) if the appeal is withdrawn by the appellant, the day after the day it is withdrawn;
    c) the day specified in the notice.
12) If there is no appeal under subsection (8), the compliance notice takes effect on the later of the following:
    a) 14 days after the notice is served on the person;
    b) the day specified in the notice.
13) An authorised officer may—
    a) withdraw a compliance notice at any time, or
    b) if no appeal is made or pending under subsection (8), extend the date specified in the notice.
14) An Essential Entity commits an offence who, without reasonable excuse, fails to comply with a compliance direction or requirement specified in a compliance notice and is liable to the fines and penalties provided in Head 37B and, or, to an Administrative Fine.
15) Withdrawal of a compliance notice under subsection (13) does not prevent the service of another compliance notice, whether in respect of the same matter or a different matter.

Explanatory Note

This Head transposes the enforcement piece of Article 32 of the Directive. In particular it allows for an authorised officer to issue compliance notices to an Essential Entity. The compliance notices will compel the Essential Entity to carry out tasks and fulfil obligations to remedy suspected breaches of this act or the security of essential systems. Failure to comply with a compliance notice can lead to a penalty under Head 37B or it can lead to the Administrative Fine process under Part 8A.

This head also provides a mechanism to appeal the notice to the District Court in the first instance who can act as an independent arbitrator in determining the necessity of the requirements of the compliance notice. This is an important mechanism that allows Essential Entities an avenue to due process and protection of their rights.

Head 37- Supervisory and enforcement measures in relation to Important Entities

1) For the purposes of this Head, the supervisory and enforcement measures as they relate to an Important Entity may only be exercised by a designated National Competent Authority once they have been made aware of alleged non-compliance of the Important Entity with this act, in particular Head 15 and Head 29.
2) For the purposes of the exercise by a designated National Competent Authority of its ex-post supervisory functions under this Act, or any regulations made under this Act, in relation to any Important Entity, an authorised officer may—
   a) give a direction to the entity requiring it, at such time or times and place or places, and in such manner, as may be specified in the direction, to allow a targeted, ex-post security audits of its processes and systems, to be conducted by an independent third party, or by the competent authority,

      and, or

   b) give a direction to the entity requiring it to give all assistance to the authorised officer or any other person nominated by the authorised officer as the Important Entity is reasonably able to give in order to conduct a targeted security scan of the entity's systems,

      and, or,

   c) give a direction to the entity requiring it, at such time and place, and in such manner, as may be specified in the direction, to produce such records as are specified in the direction that,

      i) appear necessary to the authorised officer to assess the cybersecurity risk-management measures adopted by the entity concerned,

         and, or,

      ii) appear necessary to the authorised officer to assess the implementation of cybersecurity policies,

         and, or,

      iii) appear necessary to the authorised officer to carry out their supervisory functions.

3) The authorised officer shall give a direction at section (2)(a) only where a risk assessment conducted by the National Competent Authority, or by the Important Entity, has been conducted, or where any other information causes the authorised officer to consider that there are sufficient grounds of risk to give the direction.
4) Any direction given by an authorised officer at section (2)(a) or section (2)(b) shall require the Important Entity, or any third party performing the audit, to provide any and all such information concerning the audit, as deemed necessary, to the authorised officer.
5) The costs of any security audit carried out by an independent body in compliance with section (2)(a) or (2)(b) shall be paid by the Important Entity, except in duly substantiated cases where the competent authority decides otherwise.

6) When giving a direction under section 2 (d), the authorised officer shall state the purpose of the request and specify the information requested.

Explanatory Note

This Head transposes the enforcement piece of Article 32 of the Directive. In relation to Important Entities, it empowers authorised officers of Competent Authorities to issue directions to be subjected to security audits, hand over documents and records relating to the cybersecurity provisions within the Entity, conduct security scans and provides the basis on which they can be done in an ex-post situation.

Head 37A – Compliance Notices (Important Entities)

1) An authorised officer who is of the opinion that an Important Entity is committing or engaging in, an activity or practice, or is contravening or has contravened an enactment specified in the Act, may serve, personally or by post or by electronic means, a written notice on that Essential Entity (a "compliance notice").
2) A compliance notice shall be signed and dated by the authorised officer and shall—
   a) contain a statement of the alleged contravention, the opinion referred to in subsection (6) and the reasons for that opinion, and
   b) direct the entity to adopt any measures that, in the opinion of the authorised officer, are necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation,

      and, or,

   c) direct the entity to cease any conduct that infringes this Act and desist from repeating that conduct,

      and, or,

   d) direct the entity to ensure that their cybersecurity risk-management measures comply with Head 29 of the Act or to fulfil the reporting obligations laid down in Head 15 of this Act, in a specified manner and within a specified period of time,

      and, or,

   e) direct the entity to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat,

      and, or,

   f) direct the entity to implement the recommendations provided as a result of a security audit within a specified period of time,

   g) and contain a statement that the person may appeal the notice to the District Court within 14 days after service of the notice, including information specifying –

      i) the form and manner of such an appeal, and
      ii) the service address of the National Competent Authority for purposes of notifying the National Competent Authority under subsection (6),

      and

   h) contain a statement that, if an appeal is not made in accordance with this section and within the time specified in paragraph (j), then—

i) the notice will be treated as not disputed,

ii) the Essential Entity will be deemed to have accepted the notice and have agreed to comply with the compliance direction and requirements, and

iii) any failure or refusal to so comply is a contravention of this section and the entity will be liable to the penalties as set out in Head 36B.

3) A Competent Authority can publish warnings about infringements of this Act by the Important Entity to whom it has issued a compliance notice.
4) Subject to subsection (b),
   a) a compliance notice shall be complied with within such period as may be specified in the notice which period shall not be less than 14 working days after the date of the notice.
   b) Upon the written application of the person on whom a notice is served, the period specified in the notice as the period within which that notice must be complied with may be extended by and at the discretion of the competent authority and, where the period is so extended, the compliance notice shall be complied within such extended time period.
5) An entity on whom a compliance notice has been served shall confirm in writing to the competent authority concerned that the compliance notice has been complied with as soon as practicable after so complying and in any case not later than 7 working days after the date specified in the notice by which it is to be complied with or, where the period of time has been extended under section (4), the date specified in accordance with the extension.
6) Where a person on whom a compliance notice has been served so confirms in writing under section (5) that the compliance notice has been complied with, the competent authority shall, on being so satisfied, not later than one month after the date of receipt of such confirmation, serve notice on the person concerned of compliance with the compliance notice.
7) The date specified under subsection (2)(b), (2)(d) and 2(f) shall not be earlier than the end of the period within which an appeal may be made under subsection (8).
8) If the Important Entity on whom the compliance notice is served wishes to dispute the notice, the Entity may, no later than 14 days after the notice is served and in accordance with this section and in the form and manner specified in the notice, appeal the notice to a judge of the District Court in the district court district in which the notice was served.
9) An Important Entity who appeals under subsection (8) shall at the same time notify the designated National Competent Authority of the appeal and the grounds for the appeal and the National Competent Authority shall be entitled to appear, be heard and adduce evidence on the hearing of the appeal.
10) In determining an appeal under this section, the judge may confirm, vary or cancel the compliance notice, if satisfied that it is reasonable to do so.
11) If on appeal the compliance notice is not cancelled, the notice takes effect on the later of the following:
    a) the day after the day on which the notice is confirmed or varied on appeal;
    b) if the appeal is withdrawn by the appellant, the day after the day it is withdrawn;
    c) the day specified in the notice.
12) If there is no appeal under subsection (8), the compliance notice takes effect on the later of the following:
    a) 14 days after the notice is served on the person;
    b) the day specified in the notice.
13) An authorised officer may—

a) withdraw a compliance notice at any time, or
b) if no appeal is made or pending under subsection (8), extend the date specified in the notice.

14) An Important Entity commits an offence who, without reasonable excuse, fails to comply with a compliance direction or requirement specified in a compliance notice and is liable to the fines provided in Head 37B and, or, to an Administrative Fine.
15) Withdrawal of a compliance notice under subsection (13) does not prevent the service of another compliance notice, whether in respect of the same matter or a different matter.

Explanatory Note

This Head transposes the enforcement piece of Article 33 of the Directive. In particular it allows for an authorised officer to issue compliance notices to an Important Entity. The compliance notices will compel the Important Entity to carry out tasks and fulfil obligations to remedy suspected breaches of this act or the security of essential systems. Failure to comply with a compliance notice can lead to a penalty under Head 37B or it can lead to the Administrative Fine process under Part 8A.

This head also provides a mechanism to appeal the notice to the District Court in the first instance who can act as an independent arbitrator in determining the necessity of the requirements of the compliance notice. This is an important mechanism that allows Important Entities an avenue to due process and protection of their rights.

Head 37B – Penalties for non-compliance with a Compliance Notice

1) Where an Essential Entity has not complied with enforcement measures issued pursuant to section 2, paragraphs (a) to (d) and paragraphs (f) and (g) of Head 36A, or an Important Entity has not complied with enforcement measures issued pursuant to section 2, paragraphs (a) to (d) and paragraph (f) of Head 37A, set out in a compliance notice, the designated National Competent Authority may –
   a) make an application to the High Court to declare that any natural person who is responsible for discharging managerial responsibilities at chief executive officer or who is a director of the Essential Entity, or the Important Entity, within the meaning of the Companies Act 2014 as amended, shall not act in any way, directly or indirectly, as the chief executive officer, or as a director or secretary of the Essential Entity, or the Important Entity, or exercise any managerial functions in that entity unless and until the Court is satisfied that the Essential Entity, or the important Entity, meets the requirements set out in the compliance notice,

      and, or,

   b) where the Essential Entity, or the Important Entity, operates under a license or permit issued by the National Competent Authority, temporarily suspend the license or authorisation concerning part or all of the relevant services provided or activities carried out by the Essential Entity, or the Important Entity.
2) The High Court shall make a declaration under subsection (1)(a) unless it is satisfied that—
   a) the person concerned has acted honestly and responsibly in relation to the compliance notice,
   b) he or she has, when requested to do so by the National Competent Authority, cooperated as far as could reasonably be expected in relation to the measures in the Compliance Notice and
   c) there is no other reason why it would be just and equitable that he or she should be subject to the restrictions imposed by an order under subsection (1)(a).
3) When taking any of the enforcement measures referred to in this section, the competent authority shall take account of the circumstances of each individual case and, take due account of–
   a) the seriousness of the infringement and the importance of the provisions breached, the following, inter alia, constituting serious infringement in any event:
      i) repeated violations;
      ii) a failure to notify or remedy significant incidents;
      iii) a failure to remedy deficiencies following binding instructions from competent authorities;
      iv) the obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement;
      v) providing false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting obligations laid down in [Heads 15 and 29];
   b) the duration of the infringement;
   c) any relevant previous infringements by the entity concerned;
   d) any material or non-material damage caused, including any financial or economic loss, effects on other services and the number of users affected;
   e) any intent or negligence on the part of the perpetrator of the infringement;

f) any measures taken by the entity to prevent or mitigate the material or non-material damage;
g) any adherence to approved codes of conduct or approved certification mechanisms;
h) the level of cooperation of the natural or legal persons held responsible with the competent authorities

4) The competent authority shall set out a detailed reasoning for their enforcement measures, and, before adopting such measures, the competent authorities shall -
   a) notify the Essential Entity, or Important Entity, of their preliminary findings, and
   b) allow 14 days for Essential Entity, or Important Entity, to submit observations, except in duly substantiated cases where immediate action to prevent or respond to incidents would otherwise be impeded.
5) An application to the High Court under section (1)(a) shall be on notice to the Essential Entity, or Important Entity, except in duly substantiated cases where immediate action to prevent or respond to incidents would otherwise be impeded.

Explanatory Note

Article 36 of the directive provides for penalties for non-compliance with the Directive. In this Head we are providing for the power to restrict company CEOs and Directors and other senior managers from their positions in Essential and Important Entities where there has been a non-compliance with this act. We have also provided a power for an NCA who issues a license to an entity to operate their business in the State to suspend that license until there is a compliance with the provisions in the Directive. These penalties are serious in nature but reflect the seriousness of the breaches and also reflect what is contained within the Directive.

We have provided for a mechanism to deal with these penalties through the High Court. We believe that as this deals with matters that greatly affect the operations of a company or its directors, it should be dealt with by a court of high standing. The High Court provides a sufficient level of safeguards in the implementation of these measures. It also follows the attitude adopted in the Companies Act (2014) (as amended) where all sanctions of a serious nature are dealt with by the High Court.

Head 37C – Powers of Inspection

1) For the purposes of the exercise by a designated National Competent Authority of its supervisory functions under this Act, or any regulations made under this Act, in relation to any Essential Entity, an authorised officer may—
   a) enter, at any reasonable time, and accompanied by any such other individuals or members of An Garda Síochána as deemed necessary by that officer, any premises or place or any vehicle or vessel where any activity connected with the operations of the Essential Entity take place or, in the opinion of the officer takes place, and search and inspect the premises, place, vehicle or vessel and any books, documents or records found therein,
   b) require any such person to produce to him or her any books, documents or records relating to the security of systems or associated facilities, which are in the person's power or control and, in the case of information in a non-legible form to reproduce it in a legible form, and to give to the officer such information as he or she may reasonably require in relation to any entries in such books, documents or records,
   c) secure for later inspection any such premises, place, vehicle or vessel or part thereof in which books, documents or records relating to the cyber security of the Essential Entity are kept or there are reasonable grounds for believing that such books, documents or records are kept,
   d) inspect and take extracts from or make copies of any such books, documents or records (including, in the case of information in a non-legible form, a copy of or extract from such information in a permanent legible form),
   e) remove and retain such books, documents or records for such period as may be reasonable for further examination,
   f) require the person to maintain such books, documents or records for such period of time, as may be reasonable, as the authorised officer directs,
   g) require the person to give to the officer any information which he or she may reasonably require with regard to the cybersecurity of the Essential Entity,
   h) make such inspections, tests and scans of machinery, apparatus, appliances and other equipment on the premises or vessel or at the place or in the vehicle as he or she considers appropriate,
   i) require any person on the premises or vessel or at the place or in the vehicle having charge of, or otherwise concerned with the operation of, any machinery, apparatus, appliance or other equipment (including data equipment) or any associated apparatus or material, to afford the officer all reasonable assistance in relation thereto,
   j) take photographs or make any record or visual recording of any activity on such premises or vessel, at such place or in such vehicle.
2) For the purposes of an Important Entity, an authorised officer may exercise any of the powers at section (1)(a) to (1)(j) in an ex-post situation.
3) Where an authorised officer in exercise of his or her powers under this section is prevented from entering any premises or place, an application may be made under Head 36D for a warrant to authorise such entry.
4) An authorised officer shall not, other than with the consent of the occupier, enter a private dwelling unless he or she has obtained a warrant under Head 37D authorising such entry.
5) A person to whom this section applies who—
   a) obstructs, impedes or assaults an authorised officer in the exercise of a power under this section,
   b) fails or refuses to comply with a requirement under this section,

c) alters, suppresses or destroys any books, documents or records which the person concerned has been required to produce, or may reasonably expect to be required to produce,

d) gives to the Competent Authority or to an authorised officer information which is false or misleading in a material respect, or

is guilty of an offence and is liable on summary conviction to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months or both or is liable on conviction on indictment to a fine up to €50,000 or imprisonment for a term of up to five years or both.

Explanatory Note

NIS 2 requires an ability for NCA's to conduct inspections of Essential and Important Entities. This Head gives effect to that provision. Authorised officers are empowered to arrive at the operations of an Essential or Important entities and conduct inspections to ensure compliance with this Act. Officers are not permitted to enter private residences unless by consent or under a warrant obtained from a District Court Judge under Head 37D. This head also provides for an offence of interfering with the inspection process which is in line with provisions in similar enforcement legislation.

Head 37D – Search Warrants

If a judge of the District Court is satisfied on the sworn information of an authorised officer that there are reasonable grounds for suspecting that information required by an authorised officer for the purpose of the National Competent Authority exercising its functions under this Act, or regulations made under this Act is held at any premises or place or on any vessel or in any vehicle, the judge may issue a warrant authorising the authorised officer, accompanied if the officer considers it necessary by any other individuals or members of the Garda Síochána, at any time or times, within one month from the date of issue of the warrant, on production, if so required, of the warrant, to enter, if need be by reasonable force, the premises, place, vessel or vehicle and exercise all or any of the powers conferred on an authorised officer under Head 37C .

Explanatory Note

This Head provides for the power to apply to the district court to allow authorised officer to carry out their powers of inspection under Head 37C. The option to apply for a warrant is an important provision to allow for inspections to take place where entities are not being compliant under the act.

Head 37E – Cooperation between National Competent Authorities

1) National Competent Authorities designated under this Act shall inform the relevant National Competent Authorities designated under Directive (EU) 2022/2557 (Critical Entities Resilience Directive) when exercising their supervisory and enforcement powers at Heads 36, 36A, 37B and 37C on an Essential Entity that has also been designated a critical entity under Directive (EU) 2022/ 2557(CER).
2) The relevant designated National Competent Authority under Directive (EU) 2022/2557 (CER) may request the relevant National Competent Authority under this Act to exercise their supervisory and enforcement powers at Heads 36, 36A, 37B and 37C in relation to an entity that is identified as a critical entity under Directive (EU) 2022/2557 (CER).
3) A request under section (2) shall require the National Competent Authority to conduct an initial risk assessment of the entity to determine whether it will exercise their supervisory and enforcement powers at Heads 36, 36A, 37B and 37C.
4) Competent authorities under this [Act] shall cooperate with the relevant competent authorities of the State concerned under [Regulation (EU) 2022/2554 (Digital Operational Resilience Act). In particular, competent authorities under this [Act] shall inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 (DORA)] when exercising their supervisory and enforcement powers, at Heads 36, 36A, 37, 37A, 37B and 37C, aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to [Article 31 of Regulation (EU) 2022/2554 (DORA)] with this [Act].

Explanatory Note

This Head sets out the statutory basis to allow cooperation between NCAs that have been designated under NIS2 to cooperate with NCAs that have been designated under the CER directive when they are carrying out enforcement functions on the same regulated entity. This is giving effect to provisions in Article 32 and 33 of the NIS2 Directive.

Head 38 – Security assessment

(1) A competent authority may, in relation to those sectors in respect of which it is designated as the competent authority, carry out an assessment, whether by means of a security audit or otherwise, of an entity's compliance with its obligations under [Head x and X] and for that purpose may appoint an independent person or auditor to carry out the assessment on its behalf.

(2) An authorised officer of the Competent Authority referred to in section (1) may give a direction to a designated entity, as the case may be, to provide to the competent authority —

   a. any information that the authorised officer deems necessary for that competent authority to assess the security of the network and information systems of the operator or provider, as the case may be, including documented security policies, and

   b. evidence of the effective implementation by the operator or provider, as the case may be, of security policies including the implementation of any recommendations made on foot of a security audit or other assessment.

(3) Subject to subsection (4), a person who fails to comply with a requirement under section subsection (2) to produce the required information or to provide an explanation or to make a statement shall be guilty of an offence.

(4) In any proceedings against a person in respect of an offence under subsection (1) consisting of a failure to comply with a requirement to produce the required information, it shall be a defence to prove both that—

   a. the required information was not in that person's possession or under that person's control, and

   b. it was not reasonably practicable for that person to comply with the requirement.

(5) A person who provides an explanation or makes a statement that is false or misleading in a material respect knowing it to be so false or misleading shall be guilty of an offence.

(6) A person who with notice of a direction given under section 2 destroys, mutilates, falsifies or conceals any document that is the subject of the direction shall be guilty of an offence.

(7) A person who is guilty of an offence under sections (3), (5) and (6) is liable on summary conviction to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months or both or is liable on conviction on indictment to a fine up to €50,000 or imprisonment for a term of up to five years or both.

Explanatory Note

This Head provides for competent authorities to carry out security assessments which related to the provisions regarding regular and targeted security audits carried out by an independent body or a competent authority. This section also provides for offences where the information is not provided or where the information is wilfully destroyed by a person. This is line with similar provisions in s.785 of the Companies Act (2014)

It is intended to align the provisions regarding security assessment in SI 360 of 2018 with the requirements of the NIS2 Directive.

Head 39 – Authorised officers

(1) A competent authority designated under this Act may appoint persons to be authorised officers for the purposes of this Act.

(2) A person appointed under section (1) shall, on his or her appointment, be furnished by the competent authority with a warrant of appointment and an accompanying photographic identity card and when exercising a power conferred by this Act shall, if requested by any person thereby affected, produce such warrant and identification to that person for inspection.

(3) A competent authority referred to in section (1) may terminate the appointment of an authorised officer appointed by the competent authority, whether or not the appointment was for a fixed period.

(4) An appointment as an authorised officer ceases—

a. if it is terminated under section (2),

b. if it is for a fixed period, on the expiry of that period, or

c. if the person appointed is an officer of the competent authority referred to in section (1), on the person ceasing to be such an officer.

(5) A person who falsely represents himself or herself to be an authorised officer is guilty of an offence.

(6) A person who is guilty of an offence under sections (3), (5) and (6) is liable on summary conviction to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months or both or is liable on conviction on indictment to a fine up to €50,000 or imprisonment for a term of up to five years or both.

Explanatory Note

This Head defines what an authorised officer is and how they shall be appointed by a Competent Authority. It also provides for an arrestable offence for the impersonation of an authorised officer. This recognises the seriousness of the situation where an individual may purport to be an authorised officer to attempt to gain influence over an Essential or Important Entity. The punishment is in line with provisions in the Garda Síochána Act (2005) for impersonating a member of An Garda Síochána.

Head 40 – Service of Documents

(1) Subject to sections (2) and (3), a notice, direction, certificate or any other document that is required to be served on a person by this Act shall be in writing and addressed to the person concerned by name, and may be so served to the person in one or more of the following ways:
   a. by delivering it to the person;
   b. by leaving it at the address at which the person ordinarily resides or carries on business or, in a case in which an address for service has been given, at that address;
   c. by sending it by post in a prepaid registered letter or any other form of recorded delivery service to the address referred to in [section(b)];
   d. where there is a facility for receiving the text of the notice by electronic means at the address at which the person carries on business or ordinarily resides, by transmitting the text of the notice by such means to such address, provided that the notice is also delivered in any of the other ways referred to in this paragraph;
   e. if the address at which the person ordinarily resides cannot be ascertained by reasonable enquiry and the notice relates to a premises, by delivering it to the premises or by affixing it in a conspicuous position on or near the premises.

(2) Where a notice, direction, certificate or other document under this [Act] is to be served on a person who is the owner or occupier of land or property and the name of the person cannot be ascertained by reasonable inquiry, it may be addressed to the person by using the words "the owner" or, as the case may require, "the occupier".

(3) For the purposes of this Act, a company formed and registered under the Companies Act 2014 (No. 38 of 2014) or an existing company within the meaning of that Act shall be deemed to be ordinarily resident at its registered office, and every other body corporate and every unincorporated body shall be deemed to be ordinarily resident at its principal office or place of business.

(4) Where an opinion, finding, statement or decision of a competent authority is contained in a document which—
   a. purports to have been made by or at the direction of that competent authority, and
   b. is produced in evidence by an officer of the competent authority or
   c. by an authorised officer in any proceedings,

such document shall be admissible in evidence and shall be evidence of any such opinion, finding, statement or decision in such proceedings without further proof.

Explanatory Note

This Head provides for the service of documents on a person. These provisions are taken from the original implementation of NIS under S.I 306 of 2018 and lays out the methods by which documents are to be served on entities and persons affected by the Act.

Head 41- Non-applicability of Part 8 and Part 8A

The provisions in Head 37B and all of Part 8A of this Act shall not apply to any entity designated as a public body under Head 23 of this Act.

Explanatory Note

This Head provides that the penalty provisions or enforcement procedures laid out at Head 37B or in Part 8A of this act do not apply to public bodies. The policy here is to prevent the expenditure of public money on court cases and legal fees where one State entity is seeking to impose sanctions on another. It is the belief of this Department that any non-compliance with this act can be dealt with through the Comptroller & Auditor General's Office, Ministerial Orders, Government Decision or Oireachtas Committees. The power to exempt public bodies from the penalties and sanctions provisions of the Act is provided for in the Directive.

Head 42- Infringements Entailing a Personal Data Breach

(1) Where a competent authority becomes aware in the course of supervision or enforcement that the infringement by an essential or important entity of the obligations laid down in Head 15 or 29, of this Act can entail a personal data breach, which is to be notified pursuant to section 86 of the Data Protection Act 2018, they shall, without undue delay, inform the Data Protection Commission.

(2) Where the supervisory authorities as referred to in Article 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine pursuant to Article 58(2), point (i), of that Regulation the competent authorities shall not impose an administrative fine pursuant to Head 44AG of this Act for an infringement referred to in section 1 of this Head arising from the same conduct as that which was the subject of the administrative fine under Article 58(2), point (i), of Regulation (EU) 2016/679. The competent authority may, however, impose the enforcement measures provided for in Head 37 of this Act.

(3) Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority shall inform the supervisory authority established in its own Member State of the potential data breach referred to in [section 1].

Explanatory Note

This Head transposes the relevant portions of Article 35 of the NIS 2 Directive regarding Infringements entailing a personal data breach.

Where a competent authority becomes aware in the course of supervision or enforcement that the infringement by an essential or important entity of the obligations laid down in Articles 21 and 23 of the Directive can entail a personal data breach, as defined in Article 4, point (12), of Regulation (EU) 2016/679 (GDPR) which is to be notified pursuant to Article 33 of that Regulation they shall, without undue delay, inform the supervisory authorities as referred to in Article 55 or 56 of that [Act].

Head 43 – Offence by body corporate

(1) Where an infringement, non-compliance or offence under this Act is committed by a body corporate and is proved to have been so committed with the consent or connivance of, or to be attributable to any wilful neglect on the part of, any person, being a director, manager, secretary or other officer of the body corporate, or a person who was purporting to act in any such capacity, that person, as well as the body corporate, is guilty of an infringement, non-compliance or offence and is liable to be proceeded against and punished as if he or she were guilty of the first-mentioned infringement, non-compliance or offence.

(2) Where the affairs of a body corporate are managed by its members, section (1) applies in relation to the acts and defaults of a member in connection with his or her functions of management as if he or she were a director or manager of the body corporate.

Explanatory Note

This Head provides for offences, infringements, or non-compliance by the body corporate. It is intended to align with the provision in the NIS framework that where a body corporate has committed an infringement, offence or non-compliance in the context of this act, that, where it can be proven there was knowledge on behalf of the management board of the entity of the offence, non-compliance, or infringement, that they would also be personally held accountable for the same offence.

Part 8A

Explanatory Note

Articles 34 and 36 require the Member States to implement penalties and administrative sanctions provisions for breaches of the NIS 2 Directive. This part of the scheme provides the mechanism by which NCAs may impose administrative fines on Essential and Important Entities. It comprises 49 heads divided into seven chapters and sets out the imposition of administrative sanctions and the role of adjudicators.

Head 44- Conditions for Imposing Administrative Fines on Essential and Important Entities

1) Administrative fines shall be imposed in addition to any of the measures referred to in Head 37
2) When deciding whether to impose an administrative fine and deciding on its amount in each individual case, due regard shall be given by the Competent Authority, as a minimum, to the elements provided for in [Head 37B(3)].

Explanatory Note

Heads 44 to 44AW provide for the regime to impose administrative sanctions provided under the NIS2 Directive under Article 34. In considering how to impose the regime the Department was cognisant of the need to provide for due process, fair procedures and rights of appeal. The Department also considered other legislation on the statute book which has implemented administrative sanctions from EU directives. The Communications Regulation and Digital Hub Development Agency (Amendment) Act (2023) provided a template to achieve the implementation of this regime.

Head 44A- Interpretation

In this Part—

"a Class A fine" is a fine within the meaning of the Fines Act 2010

"adjudication" means—

a) a decision by an adjudicator under Head 44AC , and
b) any decision of the adjudicator under Head 44AD on foot of that decision,

or either such decision;

"adjudicator" has the meaning given to it by HEAD 44O ;

"administrative sanction" means—

a) a requirement to cease a regulatory breach or to take specified measures to remedy the breach,
b) a requirement to pay a financial penalty, or

imposed under HEAD 44AD and "administrative sanctions proceedings" shall be interpreted accordingly;

"appeal" means an appeal under Chapter 7;

"authorised officer" shall be construed in accordance with Head 39;

"commercially sensitive information" means information the disclosure of which could reasonably be expected to—

(a) substantially and materially prejudice the commercial or industrial interests of—
  (i) the person required to provide the information,
  (ii) another person, or
  (iii) a class of persons in which a person referred to in subparagraph (i) or (ii) falls,
(b) substantially prejudice the competitive position of a person in the conduct of the person's business, profession or occupation, or
(c) substantially prejudice the financial position of—
  (i) the State,
  (ii) a Department of State,
  (iii) the Garda Síochána,
  (iv) the Permanent Defence Force within the meaning of the Defence Act 1954 ,
  (v) a local authority within the meaning of the Local Government Act 2001 , or
  (vi) a body established by or under any enactment or charter other than the Companies Act 2014 or a former enactment relating to companies within the meaning of section 5 of that Act;

"the Minister" means the minister of the relevant line department into which the NCA reports.

"notice of suspected non-compliance" has the meaning given to it by Head 44B ;

"notified person" means a person on whom a notice of suspected non-compliance has been served;

"referral report" has the meaning given to it by HEAD 44I .

Explanatory Note

This head provides for the relevant definitions of terms used in this part of the Act.

Chapter 1- Preliminary procedure

Head 44B- Notice of suspected non-compliance

1) In this Act, "notice of suspected non-compliance" means a notice in writing informing the person on whom it is served of the details of a regulatory breach of which the person is suspected.
2) Where an authorised officer suspects on reasonable grounds that a person has committed or is committing a regulatory breach that does not constitute a criminal offence the authorised officer may serve a notice of suspected non-compliance on the person.
3) A notice of suspected non-compliance shall be in such form as the National Competent Authority may specify, and shall—

    a) inform the notified person that the authorised officer suspects that the person has committed or is committing a regulatory breach,

    b) set out the grounds for the authorised officer's suspicion in sufficient detail to allow the notified person to fully respond to the notice of suspected non-compliance in accordance with subsection (5), and

    c) inform the notified person of its right to make submissions under subsection (5), and the period within which that right may be exercised.

4) The authorised officer shall, as soon as is practicable after issuing the notice of suspected non-compliance, serve on the notified person a copy of, or access to, any material relied upon by the authorised officer for the purpose of issuing the notice of suspected non-compliance, subject to such redactions as the authorised officer may consider necessary and appropriate in order to protect the rights of the parties or any other person, to protect commercially sensitive information, or for any other good and sufficient reason.
5) Subject to subsection (6), a notified person may, within such period as is specified in the notice, make written submissions to the authorised officer on the notice of suspected non-compliance.
6) Notwithstanding the period specified in the notice of suspected non-compliance in accordance with subsection (3)(c), the authorised officer may, where it is appropriate to do so in the circumstances of the case, extend the period within which written submissions may be made and shall notify the notified person in writing of the extended period.

Explanatory Note

This Head sets out that an authorised officer, who suspects that a person has committed or is committing a regulatory breach, which either does or does not constitute a criminal offence, may serve on the person a notice in writing of the details of the suspected breach.

Head 44C- Supplementary notice of suspected non-compliance

1) Where an authorised officer, having served a notice of suspected non-compliance, identifies—

   a) new or different points of fact or law, or new evidence, having a material impact on its analysis or the grounds set out in the notice of suspected non-compliance, or

   b) any error or inaccuracy in the notice of suspected non-compliance,

   the authorised officer shall serve a notice (referred to in this Act as a "supplementary notice of suspected non-compliance") on each notified person.

2) A supplementary notice of suspected non-compliance shall—

   a) be in such form as the National Competent Authority may specify,

   b) summarise the new or different points of fact or law or new evidence that have been identified by the authorised officer and the material impact of such points of fact or law or such evidence on the analysis or the grounds set out in the notice of suspected non-compliance of the authorised officer, and

   c) inform the notified person of its right to make written submissions under subsection (3), and specify the period within which that right may be exercised.

3) Subject to subsection (4), the notified person on which a supplementary notice of suspected non-compliance is served may, within such period as is specified in the supplementary notice, make written submissions to the authorised officer on the supplementary notice of suspected non-compliance.

4) Notwithstanding the period specified in the supplementary notice of suspected non-compliance in accordance with subsection (3), the authorised officer may, where it is appropriate to do so in the circumstances of the case, extend the period within which the notified person may make written submissions in accordance with that subsection and shall notify each notified person in writing of the extended period.

Explanatory Note

This Head provides that where an authorised officer who has already issued a notice of suspected non-compliance identifies new evidence which impacts said notice, or any error or inaccuracy in the notice, they shall serve a supplementary notice of suspected non-compliance on each person on which the initial notice was served.

Head 44D- NCA may revoke notice of suspected non-compliance, etc.

The National Competent Authority may revoke a notice of suspected non-compliance or a supplementary notice of suspected non-compliance.

Explanatory Note

This Head provides that the NCA may revoke a notice of suspected non-compliance or a supplementary notice of suspected non-compliance.

Head 44E- NCA may publish notice of suspected non-compliance, etc.

The National Competent Authority may (save where such publication would, in the opinion of the competent authority, prejudice the achievement of the objectives of this Act) publish a notice of suspected non-compliance or a supplementary notice of suspected non-compliance, with due regard for the protection of commercially sensitive information.

Explanatory Note

This Head provides that the NCA may publish a notice of suspected non-compliance or a supplementary notice of suspected non-compliance, with due regard for commercially sensitive information, save where such publication would, in the opinion of the NCA, prejudice the achievement of the objectives of this Act.

Head 44F- Commitments

1) A notified person may at any time prior to the date on which an adjudicator makes a decision under HEAD 44AC in relation to the regulatory breach specified in a notice of suspected non-compliance (referred to in this section as the "relevant breach"), propose to the National Competent Authority in writing measures to appropriately address the breach.

2) Where the National Competent Authority receives a proposal under subsection (1), it may—

   a) consult to the extent that it sees fit in relation to the proposal, including consulting publicly or consulting other persons,

   b) where it is of the opinion that it requires further information in order to consider the proposal, by notice in writing served on the person that made the proposal, require the person to give to it within a specified period specified information, and

   c) where it considers it necessary to do so, at any time before the proposal is made the subject of a commitment, propose to the person modifications, alterations, additions or other changes to the proposal.

3) Where the National Competent Authority is satisfied that the terms of the proposal (subject to any modifications, alterations, additions or other changes made to the proposal under subsection (2))—

   a) appropriately address the relevant breach, and

   b) are clear and unambiguous and capable of being complied with,

   it may notify the person in writing that it is willing to accept a commitment from the person in relation to the proposal.

4) Where a person enters into a commitment with the National Competent Authority in accordance with this section (referred to in this Act as a "commitment"), the National Competent Authority shall publish the commitment (save where such publication would, in the opinion of the National Competent Authority, prejudice the achievement of the objectives of this Act) on the website of the National Competent Authority, with due regard for the protection of commercially sensitive information, as soon as practicable after the notified person has entered into the commitment.

5) The National Competent Authority shall not take any further step in administrative sanctions proceedings in relation to the relevant breach as long as it is satisfied that—

   (a) the notified person is in compliance with the commitment, and

(b) that the information submitted by the notified person at the time it entered into the commitment was not incomplete, incorrect, false, or misleading in a material respect.

6) A commitment may be amended or terminated where both the notified person and the National Competent Authority agree to the amendment or termination.

7) Where the National Competent Authority is no longer satisfied that a notified person is in compliance with a commitment it shall notify the person that it intends to take further steps in the administrative sanctions proceedings and afford the person an opportunity to make submissions in relation to its compliance with the commitment.

Explanatory Note

This Head provides for a commitments procedure which allows the NCA to accept commitments from a person under investigation for a regulatory breach. The commitments concerned may require the person to take or refrain from taking particular actions. The commitments can be renegotiated by the parties. Should the commitments not be complied with, the original investigation can be continued.

Head 44G- Settlements

1. An authorised officer may, with the approval of the National Competent Authority, at any time prior to the date on which an adjudicator makes a decision under HEAD 44AC in relation to the regulatory breach specified in a notice of suspected non-compliance agree a settlement with a notified person.

2. An authorised officer may at any time refer a proposed settlement to the National Competent Authority board for its approval.

3. Where the National Competent Authority approves a settlement with a notified person, the authorised officer shall—

    a. prepare a report containing at least the following:

        i. a summary of the facts of the case;

        ii. the regulatory breach alleged against the notified person;

        iii. details of any administrative sanction to be imposed on the notified person as part of the settlement;

        iv. a statement that the National Competent Authority and the notified person consent to the imposition of the administrative sanction referred to in subparagraph (iii); and

        v. details of any other measures agreed to be taken either by the National Competent Authority or by the notified person on foot of the settlement agreement,

    b. give a copy of the report referred to in paragraph (a) to the notified person, and

    c. subject to subsection (4), refer the matter to an adjudicator for an adjudication on consent.

4. Where at the time the notified person is given a copy of the report in accordance with subsection (3)(b) where the matter has been referred for adjudication under Head 44H (b)—

    a. the authorised officer shall notify the adjudicator concerned of the withdrawal of the referral under section HEAD 44H (b), and

b. the matter shall be deemed to have been referred to an adjudicator under subsection (3)(c) for an adjudication on consent.

5. Where, following the confirmation of an adjudication on consent under HEAD 44AR (1) the notified person fails to comply with any of the terms of the settlement, the National Competent Authority may apply to the High Court for an order under subsection (6).

6. If satisfied on application to it under subsection (5) that a notified person has failed to comply with an adjudication on consent confirmed under Head 44AR(1), the High Court may make an order requiring that person to comply with the adjudication.

7. The National Competent Authority may, by summary proceedings brought in a court of competent jurisdiction, recover as a debt due to the competent authority any amount agreed to be paid by the notified person as part of a settlement confirmed by an order of the Court under HEAD 44AR(1).

Explanatory Note

This Head provides for a settlement procedure which allows the NCA to enter into a settlement agreement with any person under investigation for a regulatory breach prior to the date on which an adjudicator makes a decision under Head 44AC. The settlement agreement may be on such terms as may be agreed between the parties and would constitute a final resolution of the matter under investigation.

Head 44H- Actions by authorised officer following investigation

An authorised officer, having investigated a suspected regulatory breach, may, subject to Head 44G and with the consent of the board of the National Competent Authority—

a) close the investigation and not take any further action in respect of the matter, or
b) where the authorised officer suspects on reasonable grounds that the notified person has committed or is committing a regulatory breach, refer the matter in accordance with Head 44J for adjudication.

Explanatory Note

This Head states that following an investigation, an authorised officer may close the investigation and not take any further action in respect of the matter, or where the authorised officer suspects on reasonable grounds that the notified person has committed or is committing a regulatory breach, refer the matter for adjudication.

Head 44I- Referral report

Prior to referring a matter for adjudication an authorised officer shall prepare a report (referred to in this Act as a "referral report") containing—

a) a detailed description of the relevant facts of the case,

b) details of the regulatory breach concerned,

c) an outline of the facts and evidence on which the authorised officer is relying for the purpose of referring the matter to the board of the National Competent Authority for adjudication,

d) a summary of any submissions made by the notified person to the authorised officer during the investigation, including in response to the notice of suspected non-compliance or any supplementary notice of suspected non-compliance,

e) the authorised officer's assessment of the extent to which the notified person cooperated with the investigation, and

f) any other information that the authorised officer considers to be relevant to an adjudication.

Explanatory Note

This Head dictates that, prior to referring a matter for adjudication, an authorised officer shall prepare a referral report containing a detailed description of the relevant facts of the case, as well as details of the regulatory breach concerned.

Head 44J- Referral of matter by authorised officer to adjudicator for adjudication

(1) Where an authorised officer refers a matter for adjudication he or she shall provide the adjudicator with—

(a) the notice of suspected non-compliance served by the authorised officer under Head 44B , and any supplementary notice of suspected non-compliance served by the authorised officer under Head 44C ,

(b) the referral report,

(c) a copy of all material relied upon by the authorised officer in forming his or her opinion, and

(d) any submissions made by the notified person during the investigation.

(2) An authorised officer shall, as soon as is practicable after providing an adjudicator with the information specified in subsection (1), give the notified person—

(a) a copy of the referral report, and

(b) a copy of, or access to, any material (other than material that has already been provided to the notified person) relied upon by the authorised officer for the purpose of referring the matter for adjudication, subject to such redactions as the authorised officer considers necessary and appropriate in order to protect the rights of the parties or any other person, to protect commercially sensitive information, or for any other good and sufficient reason.

Explanatory Note

This Head provides that when an authorised officer refers a matter for adjudication, they shall furnish the adjudicator with the notice of suspected non-compliance served, as well as the referral report, a copy of all material relied upon in forming their opinion, and any submissions made by the notified person during the investigation.

Head 44K- Withdrawal by the National Competent Authority of matter referred to adjudicator

(1) A referral under Head 44G (3)(c) or Head 44H may be withdrawn by the National Competent Authority at any time before the adjudicator makes an adjudication or, as the case may be, an adjudication on consent.

(2) Where a referral is withdrawn under this section, the adjudicator shall—

(a) notify the notified person of the withdrawal, and

(b) take no further action in relation to the matter.

Explanatory Note

This Head allows for the NCA to withdraw a matter referred to an adjudicator, at any time before the adjudicator makes an adjudication.

Head 44L- Power of the National Competent Authority to share certain documents

(1) The National Competent Authority may provide a copy of any notice or document referred to in Head 44B , 44C , 44J or 44V to such other persons as the National Competent Authority considers appropriate, subject to such redactions as the Authority considers appropriate.

(2) A person that is provided with a copy of a notice or document under subsection (1) subject to redactions may appeal against the decision of the National Competent Authority to make such redactions—

(a) within 14 days of the date of service the copy of the notice or document, and

(b) by application to the adjudicator to whom the matter has been referred under Head 44J .

(3) A person who receives—

(a) a copy of a document referred to in subsection (1), or

(b) copies of materials under section Head 44B (5) or Head 44J (2).

shall not, without the prior authorisation of the National Competent Authority, disclose the existence or the content of the document or materials to any other person.

(4) A person who contravenes subsection (3) commits an offence and is liable on summary conviction to a class A fine.

Explanatory Note

This Head sets out that the NCA may provide a copy of any notice or document referred to in Heads 44B, 44C, 44J or 44V to such other persons as the NCA considers appropriate, subject to such redactions as the NCA considers appropriate.

Head 44M- Regulations and rules relating to referrals to adjudicator

(1) The Minister may prescribe the procedure for—

(a) making a referral under Head 44G (3)(c).

(b) withdrawing a referral under Head 44K , and

(c) making an application for an adjudication on consent under Head 44AR (1).

(2) The National Competent Authority may, subject to this Act and to any regulations made under subsection (1), make rules detailing the procedure for—

(a) making a referral under Head 44G (3)(c).

(b) withdrawing a referral under Head 44K , and

(c) making an application for an adjudication on consent under Head 44AR(1).

Explanatory Note

This Head provides that the Minister may prescribe the procedure for making and withdrawing a referral, and for making an application for an adjudication on consent under Head 44AR(1); and that the NCA, subject to any regulations made by the Minister, may make rules detailing the procedures stated above.

Chapter 2- Adjudicators

Head 44N- Nomination of adjudicators

(1) The National Competent Authority shall nominate persons who may be appointed by the Minister under Head 44O

(2) The National Competent Authority may nominate persons under subsection (1), including members of the authority's management board, employees and members of staff of the authority, who have, in the opinion of the authority, sufficient relevant expertise to merit such appointment whether or not the persons are members of the authority's management board or employees of the authority.

(3) The Minister shall, in a manner ensuring the independence of adjudicators in the performance of their functions, prescribe categories of persons who may be nominated and criteria, including requirements and qualifications, by which to determine whether or not a person is eligible to be nominated by the national competent authority for appointment by the Minister as adjudicators (including a Chief Adjudicator).

Explanatory Note

This Head outlines requirements for a person to be eligible for nomination as an adjudicator by the NCA; and allows for the Minister to prescribe categories, criteria, requirements, and qualifications necessary for a person to be eligible for nomination.

Head 44O- Appointment of adjudicators

(1) The Minister shall appoint persons (referred to in this Act as "adjudicators") to make adjudications.

(2) The Minister shall appoint a person nominated by the National Competent Authority under section 75 unless the Minister—

(a) is not satisfied that the nominated person meets the requirements and qualifications prescribed by the Minister, or

(b) considers that the nominated person does not have the independence necessary to be appointed as an adjudicator.

(3) The National Competent Authority shall appoint one of the adjudicators appointed under this section to be the Chief Adjudicator.

(4) The Minister may make regulations providing for the creation of a panel of adjudicators to perform the functions of adjudicators under this Act.

(5) If no Chief Adjudicator stands appointed by the National Competent Authority under this head the adjudicators standing appointed may agree that one of them perform the functions of Chief Adjudicator.

Explanatory Note

This Head provides that the Minister shall appoint a person nominated by the NCA as an adjudicator unless the Minister is not satisfied that the nominated person meets the requirements and qualifications prescribed by the Minister; or considers that the nominated person does not have the independence necessary to be appointed as an adjudicator. This section also states that the NCA shall appoint one of the appointed adjudicators as the Chief Adjudicator.

Head 44P- Independence of adjudicators

1) Adjudicators shall be independent in the performance of their functions.

2) The National Competent Authority shall put in place measures to ensure—

    a) the independence of adjudicators in the performance of their functions, and

    b) the effective implementation of, and adherence to, any regulations made under Head 44AH.

3) Where an adjudicator believes that performing any of his or her functions as an adjudicator in particular administrative sanctions proceedings would potentially create a conflict of interest, then the adjudicator shall recuse himself or herself from the proceedings in question and shall notify the National Competent Authority and the parties concerned of the recusal.

4) Where an adjudicator believes that performing any of his or her functions as an adjudicator would give rise to the perception of any potential conflict of interest, the adjudicator shall disclose that fact to the National Competent Authority and to the parties concerned in the matter with which the adjudicator is dealing, and shall, having regard to any submissions received from the person concerned or from the National Competent Authority, consider whether it is necessary to recuse himself or herself from the proceedings in question.

5) An adjudicator shall not make an adjudication where that adjudicator has been involved in any decision of the National Competent Authority whether or not to exercise any of the powers referred to in Chapter 1 or Part 8 for the purposes of an investigation in relation to the matter the subject of the adjudication.

6) An adjudicator shall not, during the period of his or her appointment, draw up or decide upon—

    a) guidelines under Head 44AH (other than subsection (1)(g)), or

    b) the policy of the National Competent Authority concerning—

        i) the referral of matters to the Director of Public Prosecutions or the making of referrals under Head 44G (3)(c) or 44J, and

        ii) administrative sanctions that may be imposed under 44AD,

    but may be consulted in the drawing up or deciding upon of such policy or guidelines, as the case may be.

7) Where a decision of a National Competent Authority referred to in subsection (5) is made as a college, or in any other manner whereby a decision of the National Competent Authority is treated as having been made by all members of the National Competent Authority management board, a member of the National Competent Authority who recused himself or herself from the process of making that decision shall, for the purposes of subsection (5), be deemed not to have been involved in that decision, provided that the recusal took place at a point and in a manner which does not compromise the independence of the member of the National Competent Authority as an adjudicator.

8) The chairperson or chief executive officer of a National Competent Authority shall not during his or her term of office serve as an adjudicator.

9) A member of the management board of a National Competent Authority may not during his or her term of office serve as Chief Adjudicator.

10) A member of a National Competent Authority or a member of staff of a National Competent Authority who is appointed as an adjudicator or is appointed to assist an adjudicator under Head 44T shall not be required by the National Competent Authority or by any other person to perform any duty, including any statutory duty, of a member of the National Competent Authority or a member of staff of the National Competent Authority or of an authorised officer or of an adjudicator the performance of which interferes with his or her independence in making an adjudication or, in the case of a person appointed to assist an adjudicator under Head 44T, the independence of an adjudicator whom he or she is assisting or may assist.

Explanatory Note

This Head provides that adjudicators shall be independent in the performance of their functions, and that the NCA shall put measures in place to ensure such independence. It also provides that an adjudicator shall recuse themselves from proceedings where a conflict of interest may arise.

Head 44Q- Regulations to ensure independence of adjudicators

(1) The Minister shall make regulations prescribing requirements to be imposed upon the National Competent Authority and adjudicators to implement Head 44P.

(2) Adjudicators shall not be involved in investigations of regulatory breaches and shall not act as authorised officers under Head 39 of this Act subject to such exceptions as the Minister may prescribe.

(3) Regulations under this section may make further provision for the independence of adjudicators (including an effective internal separation between the functions of the National Competent Authority and the functions of adjudicators) and any such regulations shall (where appropriate) include provision for—

(a) a requirement that adjudicators, and employees of the National Competent Authority tasked with assisting adjudicators, shall not communicate with authorised officers, employees and members of the National Competent Authority in respect of any proceeding relating to a regulatory breach before the National Competent Authority arising under this Act save on notice to the persons concerned in those proceedings the subject of a referral under Head 44G (3)(c) or 44I , or as otherwise permitted by regulations, which may include communications relating to investigations in which the adjudicators, and employees of the National Competent Authority tasked with assisting the adjudicators, have not been nor will be involved in any decision under Head 44J ,

(b) a requirement that documentation and other information concerning an investigation conducted under Part 8 which have been obtained by the National Competent Authority in the performance of its functions under this Act, shall not be disclosed to adjudicators that have been directed to make an adjudication in relation to that same investigation or to employees of the National Competent Authority or other persons (including any consultant or adviser) tasked with assisting such adjudicators save in accordance with this Act and upon notice to the persons concerned in any referral under Head 44G (3)(c) or 44J ,

(c) arrangements for oversight by specified members or employees of the National Competent Authority for compliance by the National Competent Authority with the provisions of head 44P ,

(d) reporting to the Minister or the National Competent Authority by specified members or employees of the National Competent Authority or by adjudicators of any breach of Head 44P and for remedying any such breach,

(e) a requirement that the National Competent Authority publish policies and implement measures sufficient to identify and manage conflicts of interest on the part of—

(i) adjudicators, and

(ii) any employee of the National Competent Authority or other person (including any consultant or adviser) tasked with assisting an adjudicator in the performance of his or her functions under this Act,

and

(f) a requirement that the Chief Adjudicator and the National Competent Authority report annually to the Minister on the National Competent Authority's compliance with the principle of independence under Head 44P and any regulations made hereunder and the policies the adjudicators or the National Competent Authority have adopted in order to do so.

Explanatory Note

This Head provides that the Minister shall make regulations prescribing requirements upon the NCA and adjudicators to implement Head 44P, and that these regulations may make further provision for the independence of adjudicators including, for example, an effective internal separation between the functions of the NCA and the functions of adjudicators.

Head 44R- Adjudicators may sit together

The powers and functions of an adjudicator shall be exercisable by each adjudicator for the time being standing appointed save that the Chief Adjudicator may direct that an uneven number of adjudicators sit together for the purpose of a particular adjudication or part of an adjudication and where the Chief Adjudicator so directs the functions of an adjudicator for that purpose shall be performed by those adjudicators sitting together.

Explanatory Note

This Head provides that the Chief Adjudicator may direct that an uneven number of adjudicators sit together for the purpose of a particular adjudication or part of an adjudication, and in such a case, the functions of the adjudicator for that purpose shall be exercised by those adjudicators sitting together.

Head 44S- Regulations in relation to adjudicators

1) The Minister shall, in a manner ensuring the independence of adjudicators in the performance of their functions, make regulations to provide for each of the following:

   (a) the term of appointment of adjudicators (including the term of appointment of a Chief Adjudicator), which term shall be specified in the instrument of appointment, and may be—

      (i) fixed and non-renewable, or

      (ii) fixed and renewable based upon objective, independently assessed competence-based criteria prescribed by the Minister under Head 44N (3).

   (b) the remuneration of the Chief Adjudicator and other adjudicators, which remuneration may—

      (i) not be reduced during the term of their appointment save in accordance with law, and

      (ii) vary depending on the category of person prescribed by the Minister under Head 44N (3) into which the adjudicator falls;

   (c) such prohibitions on remuneration of adjudicators during their term of office, by persons or bodies other than the National Competent Authority, as are necessary to ensure that actual or perceived conflicts of interest do not arise in the performance of the adjudicator's functions;

   (d) the renewal of appointment of adjudicators, including criteria for such renewal;

   (e) the resignation from office of adjudicators;

   (f) procedures and criteria whereby the revocation of appointments of adjudicators may only take place upon decision by the Government after independent assessment and recommendation by persons outside the National Competent Authority with relevant experience and expertise and where—

      (i) the adjudicator concerned has become incapable through ill-health of effectively performing his or her functions,

      (ii) the adjudicator concerned has engaged in serious misconduct, or

(iii) the National Competent Authority has been notified of an adjudicator's conflict of interest in more than one matter, which conflict of interest is assessed to be likely to continue,

without prejudice to the automatic removal from office as an adjudicator of an employee of the National Competent Authority upon cessation of that employment;

(g) the functions of the Chief Adjudicator;

(h) the rules concerning adjudications by adjudicators sitting together;

(i) the rules concerning promotion and increments of employees of the National Competent Authority who act as adjudicators;

(j) the rules concerning the tasking of any employee of the National Competent Authority to assist an adjudicator in their performance of his or her functions under this Act;

(k) the rules concerning the appointment of consultants or advisers for the purpose of assisting an adjudicator in the performance of his or her functions under this Act.

Explanatory Note

This Head states that the Minister shall, in a manner ensuring the independence of adjudicators in the performance of their functions, make regulations to provide for, among other things, the term of appointment of adjudicators, the remuneration of adjudicators, and the resignation from office of adjudicators.

Head 44T- Assistants to adjudicators

(1) The National Competent Authority may from time to time—

(a) require any employee of the National Competent Authority, or

(b) appoint such persons (including any consultant or adviser) as it considers necessary,

to assist adjudicators, or an individual adjudicator (including the Chief Adjudicator), in the performance of functions under this Act.

(2) Persons assisting an adjudicator in accordance with subsection (1) shall not provide such assistance in connection with any matter in which they have or may have a conflict of interest.

(3) The Chief Adjudicator may at any time direct that an employee of the National Competent Authority required to assist the adjudicators, or an individual adjudicator, under subsection (1)(a) in the performance of powers and functions under this Act, be reassigned by the National Competent Authority.

(4) Persons required to, or appointed to as the case may be, assist adjudicators under subsection (1) may perform other tasks on behalf of the National Competent Authority, including performing tasks in any investigation in which they have not been, and will not be, involved in assisting an adjudicator under this section, but they shall be solely responsible to the Chief Adjudicator, or to the adjudicator or adjudicators to which they have been individually assigned, in relation to providing assistance in accordance with subsection (1).

(5) Employees of the National Competent Authority who have been required to assist adjudicators under subsection (1)(a) and persons appointed by the National Competent Authority to assist adjudicators under subsection (1)(b) shall not be subject to the direction of any member or employee of the National Competent Authority, (other than, where such member or employee is the adjudicator) in relation to the performance of the functions referred to in that subsection.

(6) Nothing in subsection (5) shall preclude an employee of the National Competent Authority or other person appointed by the National Competent Authority being subject to the direction of a member or employee of the National Competent Authority in relation to the performance of functions not referred to in subsection (1)(a).

(7) Without prejudice to the responsibility of the National Competent Authority for employment and for entering into contracts and determining all matters relevant thereto, where an adjudicator has made a determination that specific assistance is required in a particular matter referred to the adjudicator for a decision under Head 44AC section 90 , the adjudicator shall be consulted on decisions concerning the appointment and assignment of a person to provide assistance to the adjudicator.

(8) The Minister may prescribe detailed requirements governing the appointment and assignment of persons to assist adjudicators under subsection (1)(b).

(9) The Minister may, where it is necessary to enable the proper functioning of the National Competent Authority, make regulations prescribing such limited exceptional circumstances in which persons referred to in subsection (5) may be subject to a direction referred to in that subsection.

Explanatory Note

This Head provides that the NCA may from time to time require any employee of the NCA, or appoint such persons as it considers necessary, to assist adjudicators in the performance of their functions, and sets out rules regarding same.

Head 44U- Effect of appointment as adjudicator on terms of employment or contract with National Competent Authority

(1) Nothing in this Part shall preclude the National Competent Authority from relying on any aspect of a contract of service or contract for services in relation to the performance or non-performance of tasks other than—

(a) the functions of an adjudicator under this Act, and

(b) the functions of a person required to assist adjudicators under Head 44T (1)(a) when assisting an adjudicator.

(2) The appointment of a person as an adjudicator shall not in itself—

(a) constitute employment by or within the National Competent Authority,

(b) constitute the holding of a position in the civil service, or

(c) otherwise create a contract between an adjudicator on the one part and the Minister or the National Competent Authority on the other part.

(3) Save in relation to the application of independence requirements to an adjudicator, nothing in this Part shall alter the terms and conditions of employment of an adjudicator who is an employee of the National Competent Authority on the date on which this section comes into operation.

(4) Save for such limited exceptions consistent with the independence of adjudicators in the performance of their functions that the Minister may prescribe, nothing in this Part shall prevent the application by the National Competent Authority of disciplinary procedures under a contract of employment save in respect of—

(a) the tasks of an adjudicator under this Act, and

(b) the tasks of a person required to assist adjudicators under Head 44T (1)(a) when assisting an adjudicator.

(5) The Minister may make regulations to give further effect to this section.

Explanatory Note

This Head provides that nothing in this Part shall preclude the NCA from relying on any aspect of a contract of service or contract for services in relation to the performance or non-performance of non-adjudication-related tasks, and that appointment of a person as an adjudicator shall not constitute employment by or within the NCA, nor should it constitute the holding of a position in the civil service.

Chapter 3- Procedure following referral to adjudicator

Head 44V- Notification by adjudicator following referral

As soon as practicable after a referral is made to an adjudicator under Head 44G (3)(c) or 44J, the adjudicator shall serve on the notified person—

a) a copy of this section,

b) in the case of a referral under Head 44G (3)(c), a notice in writing stating that the matter has been referred for an adjudication on consent under Head 44AR , and asking the person to confirm the matters set out in the report prepared in accordance with Head 44G (3)(a) within the period of 15 days from the date of service of the notice, or such further period, not exceeding 7 days, as the adjudicator may specify in the notice, and

c) in the case of a referral under Head 44J, a notice in writing stating that the person may make written submissions to the adjudicator on the referral report within the period of 30 days beginning on the date of service of the notice, or such further period, not exceeding 15 days, as the adjudicator may specify in the notice.

Explanatory Note

This Head provides that, as soon as is practicable after a referral is made to an adjudicator, the adjudicator shall serve on the notified person a copy of this section, as well as a notice in writing stating that the matter has been referred for an adjudication and inviting the person to make submissions in writing to the adjudicator on the referral report.

Head 44W- Actions following referral under Head 44G(3)(c)

Where a notified person served with a notice in accordance with Head 44V (b) confirms the matters set out in the report prepared in accordance with Head 44G (3)(a), an adjudicator may, at any time following such confirmation, impose on the person, in accordance with the report any of the following:

(a) a requirement to cease the regulatory breach or to take specified measures to remedy the breach;

(b) a financial penalty in accordance with Head 44AG ;

Explanatory Note

This Head provides that at any time after a referral under Head 44G(3)(c), an adjudicator may impose on the person a requirement to cease the regulatory breach or to take specified measures to remedy the breach or a financial penalty in accordance with section Head 44AG

Head 44X- Actions following referral under Head 44J

(1) In the case of a referral under Head 44j the adjudicator may do any of the following that he or she considers necessary to resolve an issue of fact or otherwise enable the adjudicator to make an adjudication:

(a) exercise any of the powers under head 44Z ;

(b) request further information from the person concerned;

(c) request further information from any other person, and may, for the purposes of doing so, provide, with due regard for the protection of commercially sensitive information, a copy of the referral report to the person;

(d) conduct an oral hearing.

(2) Where there is a dispute of fact which cannot be successfully resolved in accordance with paragraphs (a) to (c) of subsection (1) the adjudicator concerned shall, on the request of the notified person, conduct an oral hearing in order to resolve the dispute.

(3) Where an oral hearing takes place at which a person may make submissions to the adjudicator on the referral report, the adjudicator shall not be required to give to the person the material referred to in subsection (5).

(4) As soon as practicable after making a request under subsection (1)(c), the adjudicator shall give to the National Competent Authority, and shall, with due regard for the protection of commercially sensitive information, give to the notified person, a copy of the request.

(5) As soon as practicable after receiving any information pursuant to a request under subsection (1)(c), the adjudicator shall, with due regard for the protection of commercially sensitive information, give the National Competent Authority and the person—

(a) a copy of the information or, where commercial confidentiality means that such information cannot be provided in full, a summary of such information, and

(b) written notice stating that the National Competent Authority and the person may make written submissions to the adjudicator on the information within the period of 21 days beginning on the date of service of the notice, or such further period, not exceeding 14 days, as the adjudicator may specify in the notice.

(6) A person who receives a copy of a report under subsection (1)(c), shall not, without the prior authorisation of the adjudicator, disclose the existence or the content of the report to any other person.

(7) A person who contravenes subsection (6) commits an offence and is liable on summary conviction to a class A fine.

(8) An adjudicator may direct an employee of the National Competent Authority who has been required under Head 44T (1)(a) to assist the adjudicator in the performance of his or her functions to make any communication on his or her behalf.

Explanatory Note

This Head sets out that in the case of a referral under Head 44J, the adjudicator may do any of the following that they consider necessary to resolve an issue of fact or otherwise enable the adjudicator to make an adjudication: exercise any of the powers under Head 44Z; request further information from the person concerned; request further information from any other person; or conduct an oral hearing.

Head 44Y- Admissibility of evidence and rules for oral hearings conducted by adjudicators

(1) This section applies to an oral hearing before an adjudicator.

(2) An adjudicator may, by notice, in writing—

(a) summon a witness to appear to give evidence, or to produce before the adjudicator any books, documents or records in such person's power or control, or to do both, and

(b) require the witness to attend an oral hearing from day to day unless excused, or released from further attendance, by the adjudicator.

(3) An adjudicator may require evidence to be given on oath or affirmation, and may for that purpose—

(a) require a witness to take an oath or affirmation, and

(b) administer an oath to the witness orally or permit the witness to affirm.

(4) The oath or affirmation to be taken by a witness for the purposes of this section is an oath that the evidence the witness will give shall be true.

(5) The adjudicator may allow a witness at the oral hearing to give evidence by tendering a written statement, provided such statement is verified on oath or affirmation.

(6) Without prejudice to subsections (1) to (5), the adjudicator has the same powers, rights and privileges as a judge of the High Court when hearing civil proceedings on the occasion of that action including with respect to—

(a) the attendance and examination of witnesses on oath or affirmation or otherwise (including witnesses who are outside the State), and

(b) compelling the production (including discovery) of records or an identified category or categories of records.

(7) An oral hearing under this section may, at the discretion of the adjudicator, be held remotely (including in an online format), and evidence may be tendered as permitted by regulations or by an adjudicator.

(8) At the oral hearing before the adjudicator—

(a) an authorised officer or other representative of the National Competent Authority or any other person, with leave of the adjudicator, shall present the evidence in support of the referral, and

(b) the testimony of witnesses attending the oral hearing shall be given in accordance with this section and any regulations made under this section.

(9) A person to whom notice is given under subsection (2), or an authorised officer, may be examined and cross-examined at the oral hearing.

(10) At any oral hearing before an adjudicator, there shall be a right to cross-examine witnesses and call evidence in defence and reply.

(11) An oral hearing before an adjudicator shall be held in public unless the adjudicator is satisfied that, given the existence of special circumstances (which shall include whether information given or likely to be given in evidence is commercially sensitive information), the hearing or part of the hearing should be held otherwise than in public.

(12) If special circumstances exist (which shall include whether information given or likely to be given in evidence is commercially sensitive information), an adjudicator may impose restrictions on the reporting or distribution of information given at the hearing.

(13) The payment or reimbursement of, or of any part of, the reasonable travelling and subsistence expenses of a witness required to attend an oral hearing, is at the discretion of the adjudicator, and such expenses shall be discharged by the National Competent Authority.

(14) The rules of evidence shall apply to an oral hearing before an adjudicator save as may be otherwise prescribed.

(15) Nothing in this section compels the disclosure by any person of any information that the person would be entitled to refuse to produce on the grounds of legal professional privilege or authorises the inspection or copying of any document containing such information that is in the person's possession, power or control.

(16) The Minister may make regulations setting out further details or conditions for the receipt of evidence or the conduct of oral hearings under this section.

(17) Subject to any regulations under subsection (16), the National Competent Authority shall make rules providing for the conduct of an oral hearing under this section and shall publish such rules on the website of the National Competent Authority.

(18)Rules made under subsection (17) shall not have effect until they are published.

Explanatory Note

This Head provides that an adjudicator may, by notice, in writing, summon a witness to appear to give evidence, or to produce before the adjudicator any books, documents or records in such person's power or control, or to do both; and require the witness to attend an oral hearing from day to day unless excused, or released from further attendance, by the adjudicator.

Head 44Z- Powers of adjudicators and offences

(1) At any time after a referral under Head 44H an adjudicator may, on an application by the National Competent Authority or the notified person or of the adjudicator's own motion, where the adjudicator is satisfied that such direction is necessary for the determination of the issues before the adjudicator—

(a) direct authorised officers of the National Competent Authority, or the notified person (each of which, in this section, is referred to as a "party") to answer (whether on oath or affirmation or otherwise) an identified question or questions in whatever manner or form the adjudicator may specify,

(b) direct a party to adduce evidence or produce books, documents and records in its power or control, and

(c) direct a party to clarify any issue of fact that an adjudicator may deem necessary.

(2) An answer to a question put to a person in response to a direction under subsection (1)(a) is not admissible as evidence against the person in criminal proceedings, other than proceedings for perjury in circumstances where the contested response or information was provided on oath or affirmation.

(3) A summons issued by the adjudicator for the purpose of an oral hearing under Head 44Y may be substituted for, and is the equivalent of, any formal process capable of being issued in an action for enforcing the attendance of witnesses and compelling the production of records.

(4) A person the subject of a direction under this section shall be entitled to the same immunities and privileges in respect of compliance with any requirement referred to in this section as a witness appearing in proceedings before the Court.

(5) A person commits an offence if the person—

(a) is served with a notice under Head 44Y (2) and does not comply with that notice,

(b) is subject to a direction under subsection (1) and fails to comply with such direction,

(c) having been duly summoned to attend before an adjudicator under Head 44Y (2) fails without reasonable excuse to attend at the time and place indicated on the summons,

(d) while attending as a witness before an adjudicator at an oral hearing under Head 44Y refuses to—

(i) give evidence in the manner lawfully required by the adjudicator to be taken,

(ii) produce any record in the person's power or control that the person is lawfully required by the adjudicator to produce, or

(iii) answer any question that the person is lawfully required by the adjudicator to answer,

or

(e) while attending before the adjudicator engages in any conduct that, if the adjudicator were a court of law having power to punish for contempt, would be contempt of court.

(6) Where a person fails to comply with a requirement of an adjudicator under Head 44Y , with a direction under subsection (1), or with a summons to attend before an adjudicator, or refuses, while attending as a witness before the adjudicator, to do anything referred to in subsection (5) that the person is lawfully required by an adjudicator to do, or otherwise fails to comply with a direction of the adjudicator, the Court, on summary application by a party, on notice to that person, may—

(a) by order require the person to attend before the adjudicator or to do the thing that the person refused to do, as the case may be, within a period to be specified by the Court, and

(b) make such interim or interlocutory orders as it considers necessary for that purpose.

(7) A person commits an offence if, having been, or in anticipation of being, required to produce a book, document or record under subsection (1) or under Head 44Y (2), he or she intentionally or recklessly destroys or otherwise disposes of, falsifies or conceals such book, document or record or causes or permits its destruction, disposal, falsification or concealment.

(8) If information or evidence is provided by a person to an adjudicator in connection with any function of an adjudicator under this Part, that person commits an offence if—

(a) the information or evidence is false or misleading in a material respect, and

(b) the person knows, or ought reasonably to know, that it is false or misleading in a material respect.

(9) A person who provides any information to another person, knowing the information to be false or misleading in a material respect, or who recklessly provides any information to another person which is false or misleading in a material respect, knowing the information is to be used for the purpose of providing information to an adjudicator in connection with any of his or her functions under this Act, commits an offence.

(10)A person who commits an offence under subsection (5), (7), (8) or (9) is liable—

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 6 months or both, or

(b) on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine not exceeding €250,000 or both.

(11)Proceedings may be brought for an offence under this section regardless of whether or not an order has been made, or has been applied for, under subsection (6).

(12)The Minister may make regulations setting out further details or conditions for the exercise of the powers of adjudicators under this section.

(13)In this section, "Court" means the High Court.

Explanatory Note

This Head provides that at any time after a referral under Head 44H, an adjudicator may direct authorised officers of the NCA or the notified person to answer an identified question or questions in whatever manner or form the adjudicator may specify; or direct a party to adduce evidence or produce books, documents and records in its power or control; or direct a party to clarify any issue of fact that an adjudicator may deem necessary.

Head 44AA- Orders for costs in proceedings before adjudicator

(1) No order as to costs shall be made in proceedings before an adjudicator save that an adjudicator may in his or her discretion award the costs of proceedings before an adjudicator against a respondent person or, as the case may be, the National Competent Authority if the adjudicator finds that the person or the National Competent Authority has engaged in improper, irregular, unfair, or unsatisfactory conduct in connection with the investigation of the alleged regulatory breach or in the conduct of proceedings before the adjudicator.

(2) A requirement to pay costs under subsection (1) shall be proportionate to the nature and extent of the conduct that the person or, as the case may be, the National Competent Authority is found to have engaged in, and may be limited to a proportion of the overall costs of proceedings or to the costs of a particular part of the proceedings.

Explanatory Note

This Head provides that no order as to costs shall be made in proceedings before an adjudicator, save that an adjudicator in their discretion awards the costs of proceedings against a respondent where they are found to have committed a regulatory breach, or engaged in the investigation in an improper way; or against the NCA in the event that no regulatory breach is found or the NCA engaged in an improper way.

Head 44AB- Regulations in relation to proceedings before adjudicator

(1) The Minister may make regulations setting out detailed requirements in relation to decisions of an adjudicator under Heads 44AC and 44AD , in order to implement this section and otherwise in relation to the conduct of proceedings before an adjudicator in any matter referred to an adjudicator under Head 44J (in this section referred to as "proceedings"), having regard to the need for efficiency and the rights of the defence, including but not limited to all or any of the following:

(a) the form and manner of provision of information, records, documents, statements, admissions and evidence to be provided to the National Competent Authority or to the adjudicator;

(b) time limits to apply to the making and conduct of proceedings;

(c) the attendance of witnesses at an oral hearing;

(d) the form, and manner of making, of requests by an adjudicator for information, discovery or disclosure from a party to a proceeding, or a person other than a party;

(e) the provision by the National Competent Authority, or by an adjudicator, to a party to proceedings, or a person other than a party to proceedings, of information received by the adjudicator or the National Competent Authority;

(f) procedures for the consolidation and hearing of two or more proceedings together;

(g) procedures for the separation of proceedings;

(h) the publication on the website of the National Competent Authority of information and documents provided, for the purposes of proceedings, by a party to a proceeding or by a person other than a party to proceedings;

(i) the form and manner in which a proceeding may be withdrawn;

(j) any consequential, supplementary or transitional provisions as appear to the Minister to be necessary or expedient for the purpose of giving effect to the regulations.

(2) The National Competent Authority shall publish guidelines on the conduct of proceedings and may publish guidelines on any of the matters the subject of regulations under subsection (1).

Explanatory Note

This Head provides that the Minister may make regulations setting out detailed requirements in relation to decisions of an adjudicator under Heads 44AC and 44AD, including, for example: the form and manner of provision of information and evidence to be provided to the NCA or to the adjudicator; time limits to apply to the making and conduct of proceedings; and the attendance of witnesses at an oral hearing.

Head 44AC- Decision of adjudicator in relation to breach

(1) An adjudicator shall consider the following when making a decision in relation to a matter referred to him or her under Head 44J :

(a) the notice of suspected non-compliance served under Head 44B (and any supplementary notice of suspected non-compliance served under Head 44C);

(b) the referral report;

(c) any written submissions made by the notified person on the notice of suspected non-compliance, any supplementary notice of suspected non-compliance and the referral report;

(d) any submissions, statements, admissions, information, records or other evidence provided to the adjudicator in the course of the proceedings;

(e) any prior relevant adjudication that has been confirmed by the High Court under Head 44AR.

(2) In any matter referred to an adjudicator under Head 44J the adjudicator may make a decision as to whether, on the balance of probabilities, a person has committed or is committing a regulatory breach.

(3) Where—

(a) an adjudicator makes a decision under this section that a person has committed or is committing a regulatory breach, and

(b) the regulatory breach concerned constitutes a criminal offence,

the person found to have committed, or be committing, the regulatory breach shall not be prosecuted for the criminal offence constituted by the regulatory breach.

(4) A decision under subsection (2) shall be dated and include—

(a) the reasons for the decision,

(b) the notice of suspected non-compliance and any supplementary notice of suspected non-compliance,

(c) the evidence, including any information, records, documents, statements, admissions, evidence and written and oral submissions, considered,

(d) information regarding the right of appeal provided for under Head 44AO where a final decision has been made,

(e) the name of the person found to have committed, or to be committing, a regulatory breach, and the nature of the breach, and

(f) such other particulars or material as the adjudicator considers appropriate.

(5) For the avoidance of doubt, a decision may be made under subsection (2) or Head 44AD (1) in relation to conduct that is no longer ongoing at the time at which the decision is made.

Explanatory Note

This Head provides that an adjudicator shall consider the following when making a decision in relation to a matter referred to them under Head 44J: the notice of suspected non-compliance; the referral report; any written submissions made by the notified person on the notice of suspected non-compliance and the referral report; any information provided to the adjudicator in the course of the proceedings; and any prior relevant adjudication.

Head 44AD- Decision of adjudicator in relation to administrative sanction

(1) Where an adjudicator makes a decision under Head 44 AC (2), that a person has committed a regulatory breach he or she may, subject to this section, do one or more of the following:

(a) require the person to cease the regulatory breach or to take specified measures to remedy the breach;

(b) impose a financial penalty on the person in accordance with Head 44AG ;

(2) A decision under this section shall specify the time period within which the person is required, subject to any appeal, to cease a regulatory breach or to take specified measures to remedy the breach or to pay any financial penalty, refund or compensation.

(3) In determining the amount of any financial penalty to be imposed the adjudicator shall have regard to the matters outlined in Head 44AG.

(4) After reaching a decision under Head 44AC(2) and prior to making a decision under subsection (1), the adjudicator shall provide the National Competent Authority and the person to whom the decision relates with a copy of the decision under Head 44AC (2) and shall inform the National Competent Authority and the person of the intention of the adjudicator to do one or more of the things set out in subsection (1).

(5) The adjudicator shall invite the National Competent Authority and the person concerned to make written submissions in accordance with subsections (6) and (8).

(6) The National Competent Authority may, within a period of 15 working days from the date on which the adjudicator invites it to make written submissions in accordance with subsection (5), or within such further period as is considered appropriate by the adjudicator and specified when inviting submissions, make written submissions to the adjudicator in relation to the application of the criteria specified in section 94 , the amount of any financial penalty that may be imposed and in regard to guidelines made by the National Competent Authority under Head 44AH section 98 (1)(b) to (e).

(7) Where the National Competent Authority makes submissions in accordance with subsection (6) the adjudicator shall provide the person concerned with a copy of those submissions.

(8) The person concerned may—

(a) where the National Competent Authority does not make submissions in accordance with subsection (6), within the period of 15 working days from the date by which the National Competent Authority was invited to make submissions in accordance with that subsection,

(b) where the National Competent Authority makes submissions in accordance with subsection (6), with the period of 15 working days from the date on which the person is provided with a copy of those submissions, or

(c) within such further period as the adjudicator considers appropriate, and specifies when he or she invites written submissions from the person concerned,

make written submissions to the adjudicator in relation to the application of the criteria specified in Head 44AG, the amount of any financial penalty and in regard to guidelines made by the National Competent Authority under Head 44AH (1)(b) to (e).

(9) When making submissions in accordance with subsection (6), the National Competent Authority may, where it considers that there are, or have been, serious or repeated breaches of conditions by a person found to have committed a regulatory breach, recommend to the adjudicator in writing, that either or both the person's—

(a) general authorisation to provide electronic communications networks or services (other than number-independent interpersonal communications services), or

(b) some or all of the person's rights of use for radio spectrum and of use for numbering resources,

be suspended or withdrawn on a temporary or permanent basis.

(10) The adjudicator may by notice in writing request the person concerned to provide, in writing, within a period specified in the notice, such information as the adjudicator considers appropriate for the purpose of determining the administrative sanction to be imposed under subsection (1).

Explanatory Note

This Head outlines the actions an adjudicator may take where they have made a decision that a person has committed a regulatory breach, which include: requiring the person to cease the breach or take steps to remedy the breach and imposing a financial penalty.

Head 44AE- Adjudication to take effect when confirmed by High Court

(1) An adjudication shall take effect at the time it is confirmed by the High Court under Head 44AR subject to any order made by a court on an appeal of the adjudication or on an application for leave to appeal the adjudication.

(2) Where an adjudication has taken effect in accordance with subsection (1) any sanction, including any financial penalty, imposed by such adjudication may be enforced without the need for any further judgment of a court.

(3) Where an adjudication has taken effect in accordance with subsection (1) any financial penalty imposed by such adjudication may be enforced by the National Competent Authority as a judgment debt.

(4) Where a person fails to comply with an administrative sanction imposed by an adjudication that has taken effect in accordance with subsection (1) the High Court may, on an application to it by the National Competent Authority in that behalf—

(a) compel compliance with the adjudication and any administrative sanction imposed, or

(b) grant any injunctive relief that the Court considers necessary.

(5) The Court may not require the National Competent Authority to give an undertaking as to damages as a condition of granting any injunctive relief under subsection (4)(b).

Explanatory Note

This Head provides that an adjudication shall take effect at the time it is confirmed by the High Court under Head 44AR subject to any order made by a court on an appeal of the adjudication or on an application for leave to appeal the adjudication.

Head 44AF- Notice of adjudication

(1) As soon as practicable after the adjudicator has made a decision under Head 44AD , the adjudicator shall provide the National Competent Authority with the decision.

(2) The National Competent Authority shall within 7 days of receipt of the decision of the adjudicator under Head 44AD give notice in writing of the decision to the person concerned.

(3) The notice under subsection (2) shall—

(a) include a copy of the decision of the adjudicator under Head 44AC (2).

(b) state that, in so far as it imposes any administrative sanction, the adjudication shall not take effect unless it is confirmed by the Court in accordance with Head 44AR, and

(c) state that, if the person does not appeal any administrative sanction imposed by the decision under HEAD 44AO , the National Competent Authority shall, as soon as is practicable after the expiration of the period for the making of such an appeal, make an application for confirmation of the adjudication in accordance with Head 44AR.

(4) The National Competent Authority may provide a copy of a notice referred to in subsection (2) to a person other than the person concerned where it considers it appropriate to do so.

(5) A copy of the adjudication shall be published by the National Competent Authority.

(6) A decision referred to in subsection (1) and a copy of the adjudication referred to in subsection (3) may contain such redactions as the adjudicator considers necessary and appropriate, in respect of subsection (1) on his or her own motion, or in respect of subsection (2) or (3) upon application of the National Competent Authority or any of the persons concerned—

(a) to protect commercially sensitive information,

(b) to protect the rights of the person concerned or any other person, or

(c) for any other good and sufficient reason.

(7) A person who receives a copy of a notice under subsection (2) prior to the publication of the adjudication shall not, without the prior authorisation of the adjudicator, disclose the existence or the content of the notice to any other person.

(8) A person who receives a copy of a notice under subsection (2) that contains material redacted from publication under subsection (6) shall not, without the prior authorisation of the adjudicator, disclose the content of the redacted material to any other person.

(9) A person who fails to comply with subsection (7) or (8) commits an offence and is liable—

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 6 months or both, or

(b) on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine not exceeding €250,000 or both.

Explanatory Note

This Head provides that as soon as is practicable after the adjudicator has made a decision under Head 44AD, they shall provide the NCA with the decision. Within 7 days of the receipt of the decision, the NCA shall give notice in writing of the decision to the person concerned.

Chapter 4- Imposition of administrative sanctions

Head 44AG- Requirement to pay financial penalty

(1) When determining the amount of a financial penalty, an adjudicator shall have regard to—

(a) the need to ensure that the financial penalty is—

(i) appropriate,

(ii) effective,

(iii) proportionate to the regulatory breach, and

(iv) dissuasive (including whether it will act as a sufficient deterrent to ensure that any similar regulatory breach will not occur in the future),

(b) the seriousness of the regulatory breach,

(c) the extent of any failure by the person to cooperate with the investigation concerned, whether or not such failure is prosecuted,

(d) any excuse or explanation offered by the person for the regulatory breach or failure to cooperate with the investigation concerned,

(e) any gain (financial or otherwise) made, or loss avoided, by the person, or by any other person in which the first-named person has a financial interest, as a consequence of the regulatory breach,

(f) the amount of any loss suffered, or costs incurred, by any person as a result of the regulatory breach,

(g) the effect of the regulatory breach on other operators, consumers and other end-users,

(h) the duration of the regulatory breach,

(i) the number of times the regulatory breach has occurred,

(j) whether or not the regulatory breach continued after the person was served with a notice of suspected non-compliance,

(k) where applicable, the absence, ineffectiveness or repeated failure of internal mechanisms or procedures of the person intended to prevent such a regulatory breach from occurring,

(l) where applicable, the extent and timeliness of any steps taken to end the regulatory breach and any steps taken to remedy the consequences of the regulatory breach,

(m) whether a financial penalty in respect of a similar regulatory breach has already been imposed on the person by a court or a competent authority, including by the National Competent Authority,

(n) any precedents set by a court or a competent authority, including the National Competent Authority, in respect of a similar regulatory breach,

(o) any specific factors, criteria or methodology relevant to paragraphs (a) to (o) prescribed by the Minister for the purposes of this subsection, and

(p) any guidelines made by the National Competent Authority under Head 44AAH in respect of the calculation of the amount of a financial penalty.

(2) The National Competent Authority may make rules for the purposes of the implementation of this section.

(3) The adjudicator may, having imposed a financial penalty on a person (in this subsection referred to as the "sanctioned person") in accordance with this section and where he or she considers that it is necessary to do so in order to ensure that the penalty be appropriate, effective, proportionate and dissuasive, impose the penalty (whether jointly with or separately to the sanctioned person) on either or both of the following:

(a) a subsidiary of the sanctioned person;

(b) a person of which the sanctioned person is a subsidiary.

(4) The following shall apply for the purposes of this section:

(a) "subsidiary" shall have the same meaning as it has in section 7 of the Companies Act 2014 ;

(b) where a person is a partnership, for the purposes of the application to it of the definition of "subsidiary"—

(i) references to voting rights attaching to shares in a company shall be construed as references to votes or other rights exercisable by the partners in a partnership giving those partners the potential to exercise control or dominant influence over the activities of the partnership, and

(ii) references to a company's constitution shall be construed as references to any agreement or practice governing or concerning the operation of the partnership;

(c) where a person is an unincorporated association, for the purposes of the application to it of the definition of "subsidiary undertaking"—

(i) references to voting rights attaching to shares in a company shall be construed as references to votes or other rights exercisable by the members of the unincorporated association giving those members the potential to exercise control or dominant influence over the activities of the unincorporated association, and references to a company's constitution shall be construed as references to the constitution or of any agreement or practice governing or concerning the operation of the unincorporated association, and

(ii) references to a company's constitution shall be construed as references to the constitution or of any agreement or practice governing or concerning the operation of the unincorporated association.

(5) The maximum amount of a financial penalty that an adjudicator may impose on a person under this Part in respect of a regulatory breach shall be—

(a) in the case of an Essential Entity that infringes under Head 15 or Head 29, and subject to paragraphs (2) and (3) of Article 34 of the Directive, the greater of €10 million and of at least 2 per cent of the worldwide turnover of the Essential Entity in the financial year ending in the year immediately before the financial year in which the regulatory breach last occurred, and

(b) in the case of an Important Entity that infringes under Head 15 or Head 29, and subject to paragraphs (2) and (3) of Article 34 of the Directive, the greater of €7 million and of at least 1.4 per cent of the worldwide turnover of the Essential Entity in the financial year ending in the year immediately before the financial year in which the regulatory breach last occurred, and

Explanatory Note

This Head sets out the criteria an adjudicator shall have regard to when determining the amount of a financial penalty, including, amongst other things, the need to ensure that the financial penalty is appropriate, effective, and proportionate to the regulatory breach. It also provides that the

maximum amount of a financial penalty that an adjudicator may impose on an Essential Entity shall be the greater of €10 million and 2 per cent of the total worldwide turnover of the entity in the financial year preceding the imposition of the financial penalty, or in the case of an Important Entity, the greater of €7 million and 1.4 per cent of the total worldwide turnover in the financial year preceding the imposition of the financial penalty.

Head 44AH- Guidelines

(1) The National Competent Authority may, subject to this Act and any regulations and rules made under this Act, and having regard to the fairness and efficiency of the procedures under this Part, prepare and make guidelines in relation to any matter provided for by or under this Part, including—

(a) the conduct of oral hearings,

(b) the imposition of administrative sanctions (including the factors applicable to any financial penalty to be imposed under Head 44AD, and the method of calculation of financial penalties),

(c) the decision to carry out an investigation where there is evidence of a breach and the conduct of such investigations, including the content of referral reports and other reports of authorised officers,

(d) the general policies of the National Competent Authority.

(2) In making an adjudication, subject to this Act and any regulations and rules made under this Act, an adjudicator shall apply guidelines made and published by the National Competent Authority under subsection (1) unless the adjudicator considers that there is a good and substantial reason not to do so.

(3) The National Competent Authority may amend or revoke guidelines made under subsection (1).

(4) The National Competent Authority shall publish any guidelines made under subsection (1), and any amendment to or revocation of those guidelines.

Explanatory Note

This Head establishes that the NCA may prepare and make guidelines in relation to any matter provided for in or under this Part, including, amongst other things, the conduct of oral hearings, the imposition of administrative sanctions, the award of compensation, and the award of refunds.

Head 44AI- Regulations in relation to certain matters

The Minister may provide in regulations for any matter referred to in paragraphs (a) to (d) of Head 44AH (1).

Explanatory Note

This Head states that the Minister may provide in regulations for any matter referred to in paragraphs (a) to (d) of Head 44AH(1).

Chapter 5- Admissibility of certain evidence

Head 44AJ- Admissibility of evidence before National Competent Authority

(1) The type of proof that is admissible as evidence in proceedings under this Part (whether criminal or civil, including proceedings before the National Competent Authority or an adjudicator) shall include relevant documents, oral statements, electronic messages, recordings and all other objects containing information, irrespective of the form it takes and the medium on which information is stored, provided that the evidence referred to would have been admissible before a court were it before a court.

(2) If a document contains a statement by a person specified in subsection (3) asserting that an act has been done, or is, or was, proposed to be done, by another person, being an act that relates to a regulatory breach (the "relevant act") then subject to the conditions specified in subsection (4) being satisfied, that statement shall be admissible in proceedings in respect of the regulatory breach as evidence that the relevant act was done by that other person or was proposed (at the time the statement was made, or, as the case may be, at a previous time) to be done by him or her.

(3) The person referred to in subsection (2) is a person who has done an act of the kind referred to in that subsection in relation to the regulatory breach (whether or not the same as the act which the other person referred to in that subsection is alleged to have done or proposed to do).

(4) The conditions referred to in subsection (2) are that the document referred to in that subsection—

(a) has come into existence before the commencement of the proceedings under this Act in which it is sought to tender the document in evidence, and

(b) has been prepared otherwise than in response to any enquiry made or question put by a member or officer of the National Competent Authority, a member of the Garda Síochána, an officer of a European National Competent Authority, or an authorised officer relative to any matter the subject of those proceedings.

(5) In estimating the weight, if any, to be attached to evidence admitted by virtue of this section, regard shall be had to all the circumstances from which any inference can reasonably be drawn as to its accuracy or otherwise.

(6) Where the proof admitted in evidence by virtue of this section comprises a statement by a person—

(a) any evidence which, if the person who made the statement had been called as a witness, would have been admissible as relevant to his or her credibility as a witness shall be admissible for that purpose,

(b) evidence may, with the leave of the court or adjudicator seised of the proceedings, be given of any matter which, if that person had been called as a witness, could have been put to him or her in cross-examination as relevant to his or her credibility but of which evidence could not be adduced by the cross-examining party, and

(c) evidence tending to prove that that person, whether before or after making the statement, made (whether orally or not) a statement which is inconsistent with it shall, if not already admissible by virtue of any rule of law or other enactment, be admissible for the purpose of showing that he or she has contradicted himself or herself.

(7) Nothing in this section shall prejudice the admissibility in any proceedings under this Act before a court or an adjudicator of any document, as evidence of any matters stated in it—

(a) that is so admissible by virtue of any rule of law or other enactment, or

(b) in respect of adjudicators, that would be admissible before a Court hearing civil proceedings by virtue of any rule of law or other enactment.

(8) The provisions of Chapter 3 of the Civil Law and Criminal Law (Miscellaneous Provisions) Act 2020 shall apply to proceedings under this Act.

Explanatory Note

This Head provides that the type of proof that is admissible as evidence in proceedings under this Part shall include relevant documents, oral statements, electronic messages, recordings and all other objects containing information, irrespective of the form it takes and the medium on which information is stored.

Chapter 6 - Restrictions on disclosure of certain information

Head 44AK- Restrictions on disclosure of certain information

(1) Where an authorised officer requires a natural person to provide a statement or admission on the basis of measures referred to in applicable provisions, any such statement or admission may not be admissible in evidence against that person in criminal proceedings or for perjury where such statement or admission was provided under oath.

(2) Subject to subsection (3), and save in accordance with law, an adjudicator, an authorised officer, the National Competent Authority and its respective servants or agents shall not, without reasonable excuse, disclose to any person—

(a) any confidential information obtained by virtue of the exercise of powers conferred by or under this Act, or

(b) any information obtained by virtue of the exercise of powers conferred by or under this Part in relation to an investigation under this Part where that information was given under power of compulsion.

(3) Notwithstanding subsection (2) an adjudicator, the National Competent Authority and its servants or agents may disclose information obtained by virtue of the exercise of powers conferred by or under this Act where such disclosure is—

(a) permitted by this Act,

(b) otherwise permitted by law, or

(c) duly authorised by the National Competent Authority or an adjudicator in the performance of his or her functions.

(4) Information provided to any person pursuant to subsection (3) may contain such redactions as an adjudicator or the National Competent Authority or an authorised officer may consider necessary and appropriate—

(a) to protect commercially sensitive information,

(b) to protect the rights of the parties or any other person, or

(c) for any other good and sufficient reason.

(5) A person who contravenes subsection (2) commits an offence and is liable, on summary conviction, to a class A fine or imprisonment for a term not exceeding 6 months, or both.

(6) The following categories of information obtained by a party during investigations by an authorised officer, or administrative sanctions proceedings before an adjudicator under this Act, shall not be used by that party in proceedings before a court prior to the authorised officer or the National Competent Authority or an adjudicator, as the case may be, having closed such proceedings with respect to all parties under investigation, whether by making a decision under Head 44AC or Head 44AD :

(a) information that was prepared by persons specifically for investigations by an authorised officer or administrative sanctions proceedings before an adjudicator;

(b) information that an authorised officer or an adjudicator has drawn up and sent to the parties in the course of an investigation or administrative sanctions proceedings;

(c) settlement submissions that have been withdrawn.

Explanatory Note

This Head establishes that where an authorised officer requires a natural person to provide a statement or admission on the basis of measures referred to in applicable provisions, any such statement or admission may not be admissible in evidence against that person in criminal proceedings or for perjury where such statement or admission was provided under oath.

Head 44AL- Confidentiality rings

(1) Where the National Competent Authority or an adjudicator provides, or otherwise makes available, a document to any person, it may specify and so notify the person concerned that such document, or such part of the document as it may specify, is provided subject to this section.

(2) A document, or part of a document, provided subject to this section may not be viewed by, or shared with, any person other than one or more of the following, as the National Competent Authority may specify:

(a) the person to whom the document is provided or otherwise made available;

(b) a legal adviser, or other professional adviser, of the person to whom the document is provided or otherwise made available;

(c) such other person as the National Competent Authority may specify.

(3) A person who allows a document provided to the person subject to this section to be viewed by, or shared with, a person other than in accordance with this section commits an offence and is liable, on summary conviction, to a class A fine or imprisonment for a term not exceeding 6 months or both.

Explanatory Note

This Head provides that where the NCA or an adjudicator provides a document to any person, it may specify and so notify the person concerned that such document, or such part of the document as it may specify, may not be viewed by, or shared with, any person other than as the NCA may specify.

Chapter 7- Appeals, confirmation and judicial review of certain decisions

Head 44AM- Interpretation (Chapter 7 of Part 8)

In this Chapter, “Court” means the High Court.

Explanatory Note

This Head states that in this Chapter, “Court” means the High Court.

Head 44AN- Decisions reviewable only by appeal under this Chapter

1) An adjudication shall not be challenged, including as to its validity, other than by way of an appeal under Head 44AO .

2) For the avoidance of doubt, in respect of a decision under Head 44AC or Head 44AD, no proceeding (including an application for judicial review whether in accordance with Head 44AU or otherwise) may be brought before the courts other than an appeal under Head 44AO in the case of a decision under Head 44AC or Head 44AD or an application to have the decision confirmed under Head 44AR.

Explanatory Note

This Head states that an adjudication shall not be challenged, including as to its validity, other than by way of an appeal under Head 44AO

Head 44AO- Appeal against adjudication

(1) A person the subject of an adjudication may appeal to the Court against that adjudication not later than 28 days after the date of service of the notice under Head 44AF (2).

(2) On application, the Court may extend the period within which an appeal may be brought under subsection (1), where it is satisfied—

(a) that there is exceptional, good and sufficient reason for doing so,

(b) that the circumstances that resulted in the failure to bring an appeal within the period provided for in subsection (1) were outside the control of the applicant for the extension, and

(c) where an application for confirmation has been brought under Head 44AR, that the Court has neither heard nor determined such application.

(3) Where an application for confirmation has been brought pursuant to Head 44AR in relation to an adjudication the subject of an appeal under this section, the Court may, upon application or of its own motion, stay the proceedings under Head 44AR.

(4) Where the Court confirms an adjudication that imposes an administrative sanction, or substitutes its own decision for the adjudication of an adjudicator and, as part of such adjudication, imposes an administrative sanction, the Court may set a time limit for the payment of any financial penalty, compensation or refund required to be paid.

Explanatory Note

This Head provides that a person the subject of an adjudication may appeal to the Court against that adjudication not later than 28 days after the date of service of the notice.

Head 44AP- Conduct of appeals

(1) The respondent to an appeal shall be the National Competent Authority.

(2) A person that brings an appeal -

(a) may include in such appeal or application, as the case may be, any ground that could, but for Head 44AN , be relied upon by the appellant in an application seeking judicial review, and

(b) shall, on the same date as it makes such appeal or application, as the case may be, notify the respondent of the fact that it has made the appeal or application, and of the grounds on which it has made the appeal or application.

(3) The Court may, for the purpose of ensuring the efficient, fair and timely determination of an appeal, give directions in respect of the conduct of the appeal.

(4) An appellant shall, when making an appeal precisely state all of the grounds in law and fact upon which the appeal is made and shall provide to the Court all of the documents and evidence which it is alleged support the granting of the appeal or upon which the appellant intends to rely to support those grounds.

(5) A party to an appeal other than the appellant shall, when responding to an appeal, state all of the grounds upon which he or she responds to the appeal and provide to the Court all of the documents and evidence upon which he or she intends to rely to support those grounds.

(6) Subject to subsection (7), a party to an appeal shall not be entitled during the course of an appeal to make submissions to the Court other than submissions related to the grounds stated, or documents and evidence provided under subsections (4) and (5).

(7) The Court may, upon application and where it considers it necessary for the fair and proper determination of an appeal, require or permit a party to an appeal to—

(a) make submissions to the Court other than submissions related to the grounds stated or documents and evidence provided under subsections (4) and (5), and

(b) provide documents or evidence to the Court other than documents or evidence provided under subsections (4) and (5).

(8) Notwithstanding subsection (7), the Court shall refuse to consider submissions, documents or evidence where it considers that—

(a) the submissions, documents or evidence are not relevant to the appeal, or

(b) it is appropriate to do so in order to avoid undue repetition of submissions.

(9) Where the Court has granted leave to deliver additional submissions, documents or evidence on an application under subsection (7), the Court shall give directions as to the scope, form and time-frame for delivery of such additional submissions, documents or evidence.

(10) The Court may receive evidence by oral examination in court, by affidavit, or by deposition taken before an examiner or a National Competent Authority.

(11) The Court, on hearing an appeal against a decision, may consider—

(a) whether the jurisdiction existed to make the decision,

(b) whether the law was correctly applied in reaching the decision,

(c) whether the decision is supported by the evidence including evidence admitted in accordance with subsection (7), and

(d) in the case of an appeal against an adjudication, whether an administrative sanction was imposed as part of the adjudication that was appropriate, effective, proportionate and dissuasive.

(12) In considering an appeal, the Court shall have regard to—

(a) the record of the decision the subject of the appeal,

(b) the grounds stated by the parties to the appeal, and documents and evidence relied upon by the parties to support those grounds, under subsections (4) and (5), and

(c) any submissions, documents or evidence admitted under subsection (7).

(13) The Court may, on the hearing of an appeal against a decision—

(a) confirm the decision, or

(b) where it is satisfied by reference to the grounds of appeal that a serious and significant error of law or fact, or a series of minor errors of law or fact which when taken together amount to a serious and significant error, was made in making the decision, or that the decision was

made without complying with fair procedures, annul the decision in its totality or in part, and—

(i) remit the decision for reconsideration by the adjudicator subject to such directions as the Court considers appropriate, including, in the case of a decision by an adjudicator, whether the matter should be reconsidered by another adjudicator, or

(ii) vary the decision and substitute such other decision as the Court considers appropriate.

(14)The Court shall, in determining an appeal act as expeditiously as possible consistent with the administration of justice.

Explanatory Note

This Head sets out the procedure for appeals under this Part. It provides that on hearing an appeal, the Court may confirm the decision, or, where it is satisfied by reference to the grounds of appeal that a serious and significant error of law or fact, or a series of minor errors of law or fact which when taken together amount to a serious and significant error, was made in making the decision, or that the decision was made without complying with fair procedures, annul the decision in its totality or in part.

Head 44 AQ- Orders for costs by Court on appeal

The Court may in its discretion award the costs of an appeal as if Head 44AA applied to such an award.

Explanatory Note

This Head provides that the Court may in its discretion award the costs of an appeal as if Head 44AA applied to such an award.

Head 44 AR- Court confirmation of adjudication

(1) Where a person does not appeal to the Court against an adjudication within the period provided for in section Head 44AO (1) the National Competent Authority shall, subject to subsection (11), as soon as practicable after the expiration of the period allowed for such an appeal, make an application to the Court for the confirmation of that adjudication.

(2) An application by the National Competent Authority under subsection (1) shall include a copy of the adjudication together with the documents and evidence that were before the adjudicator which are referred to in that adjudication, and may include any other documents and evidence which were before the adjudicator.

(3) Notice of an application under subsection (1) shall be served by the National Competent Authority on the person the subject of the adjudication within 7 days of the National Competent Authority lodging the application in Court.

(4) The notice referred to in subsection (3) shall, where possible, specify the time fixed by the Court for the hearing of the application, and shall enclose copies of all the papers lodged in Court in relation to the application under subsection (1).

(5) The Court shall, on the hearing of an application under subsection (1), confirm the adjudication the subject of the application unless the Court, on the basis of the findings of fact in the adjudication (which are to be accepted as final by the Court), determines that—

(a) the adjudication contains an error of law which is—

(i) manifest from the record of the adjudication, and

(ii) fundamental so as to deprive the adjudication of its basis,

or

(b) the administrative sanction imposed was manifestly—

(i) disproportionate,

(ii) in excess of the sanction required to be dissuasive,

(iii) in excess of the sanction required to be effective, or

(iv) in excess of the sanction required to be appropriate.

(6) The Court—

(a) where it makes a determination referred to in subsection (5)(a), or both a determination referred to in subsection (5)(a) and a determination referred to in subsection (5)(b), in relation to an application under subsection (1), shall remit the matter for reconsideration by an adjudicator, subject to such directions as the Court considers appropriate including, as the Court sees fit, directions as to whether or not—

(i) the adjudicator should be limited to reconsidering a specific aspect of an adjudication, and

(ii) the matter should be reconsidered by another adjudicator,

and

(b) where it makes a determination referred to in subsection (5)(b), but does not make a determination referred to in subsection (5)(a), in relation to an application under subsection (1) may—

(i) order either or both that a lesser amount be substituted for the amount of the financial penalty, compensation or refund, and that any suspension or withdrawal of authorisation or rights of use specified in the adjudication be reduced or removed, and confirm the adjudication subject to such substitution, and

(ii) where the Court does not make an order referred to in subparagraph (i) and considers that the interests of justice so require, remit the matter for reconsideration by an adjudicator, subject to such directions as the Court considers appropriate including, as the Court sees fit, directions as to whether or not—

(i) the adjudicator should be limited to reconsidering a specific aspect of an adjudication, and

(ii) the matter should be reconsidered by another adjudicator.

(7) The Court shall hear the application under subsection (1) on the evidence before the adjudicator.

(8) The Court shall, in determining an application under subsection (1), act as expeditiously as possible consistent with the administration of justice.

(9) The Court may in its discretion award the costs of an application under this section as if Head 44AA applied to such an award.

(10) Where the Court confirms or substitutes its own decision for the decision of an adjudicator imposing a requirement to cease a regulatory breach, a requirement to take specified measures to remedy the breach, a financial penalty or a requirement to pay compensation or a refund, the Court may set a time limit for the requirement to be carried out or the payment of the financial penalty or compensation or refund concerned.

(11) The National Competent Authority shall, prior to making an application under subsection (1), seek the consent in writing of the person to the confirmation of the adjudication of the adjudicator.

(12) Where a person consents in writing to the adjudication, the application under subsection (1) (and any remaining steps in such application) may be made ex parte.

Explanatory Note

This Head provides that where a person does not appeal to the Court against an adjudication within the period provided for the NCA shall, as soon as is practicable after the expiration of the period allowed for such an appeal, make an application to the Court for the confirmation of that adjudication. This section further sets out the procedure regarding the above.

Head 44AS- Publication of adjudication

The National Competent Authority shall publish an adjudication confirmed by the Court under Head 44AR (save where such publication would, in the opinion of the National Competent Authority, prejudice the achievement of the objectives of this Act) subject to such redactions as the National Competent Authority may consider necessary and appropriate in order to protect the rights of the parties or any other person, to protect commercially sensitive information, or for any other good and sufficient reason, on the website of the National Competent Authority as soon as practicable after the adjudication is confirmed.

Explanatory Note

This Head provides that the NCA shall publish an adjudication confirmed by the Court under Head 44AR.

Head 44AT- Adjudicator may refer question of law to Court

(1) An adjudicator may, on her or his own initiative or at the request of the National Competent Authority or a person the subject of a referral under Head 44J , refer to the Court for decision by way of case-stated a question of law arising at a hearing on a referral under Head 44J .

(2) Where a question has been referred under subsection (1), the adjudicator shall not, in relation to a referral under Head 44J to which the hearing relates—

(a) make a decision under Head 44AC or 44AD to which the question is relevant while the reference to the Court is pending, or

(b) proceed in a manner, or make a decision under Head 44AC or 44AD , that is inconsistent with the Court's decision on the question.

(3) Where a question is referred to the Court under subsection (1)—

(a) the adjudicator shall send to the Court all documents before the adjudicator that are relevant to the matter in question, and

(b) at the end of the proceeding in the Court in relation to the reference, the Court shall cause the documents to be returned to the adjudicator.

Explanatory Note

This Head provides that an adjudicator may, on their own initiative or at the request of the NCA or a person the subject of a referral under Head 44J, refer to the Court for decision by way of case-stated a question of law arising at a hearing under Head 44J. This section further sets out the procedure regarding same.

Head 44AU- Judicial review

(1) The validity of a decision made or an act done by the National Competent Authority (including by an authorised officer or adjudicator) in the performance of a function under this Act (whether such function is performed by way of powers conferred by or under this Act or otherwise) shall not be challenged other than—

(a) by way of an application for judicial review under Order 84 of the Rules of the Superior Courts (S.I. No. 15 of 1986) (in this section referred to as "Order 84"), and in accordance with this section, or

(b) in accordance with a process provided for in this Act by which the validity of such decision or act may be challenged.

(2) Notwithstanding Head 44AN , a person affected by, but not the subject of, a decision under Head 44AC or 44AD may, not later than 14 days after the decision is published, apply to the Court by way of an application for judicial review under Order 84 and in accordance with this section.

(3) At any time after the bringing of an application for leave to apply for judicial review of any decision or other act to which subsection (1) applies and which relates to a matter for the time being before the National Competent Authority (including a matter before an adjudicator), the National Competent Authority may apply to the Court to stay the proceedings pending the making of a decision by the National Competent Authority (including a decision by an adjudicator) in relation to the matter concerned.

(4) On the making of an application to stay proceedings referred to in subsection (3), the Court may, where it considers that the matter before the National Competent Authority (including an adjudicator and an authorised officer) is within the jurisdiction of the National Competent Authority (including an adjudicator and an authorised officer), make an order staying the proceedings concerned on such terms as it thinks fit.

(5) Subject to subsection (6), an application for leave to apply for judicial review under Order 84 in respect of a decision or other act to which subsection (1) applies shall be made in respect of a decision made or an act done under Chapters 1 to 6 not later than 28 days from the date on which the notice of the decision or act was first sent or published as the case may be or, if notice of the decision or act was not sent or published, from the date on which the person or persons became aware of the decision or act.

(6) The Court may extend the period provided for in subsection (5) within which an application for leave referred to in that subsection may be made but shall only do so if it is satisfied that—

(a) there is good and sufficient reason for doing so, and

(b) the circumstances that resulted in the failure to make the application for leave within the period so provided were outside the control of the applicant for the extension.

(7) An application for leave under this section shall be made by motion ex parte and shall be grounded in the manner specified in Order 84 in respect of an ex parte motion for leave.

(8) The Court hearing the ex parte application for leave may decide, having regard to the issues arising, the likely impact of the proceedings on the National Competent Authority or the person concerned or another party, or for other good and sufficient reason, that the application for leave should be conducted on an inter partes basis and may adjourn the application on such terms as it may direct in order that a notice may be served on that person.

(9) If the Court directs that the leave hearing is to be conducted on an inter partes basis it shall be by motion on notice (grounded in the manner specified in Order 84 in respect of an ex parte motion for leave)—

(a) if the application relates to a decision made or other act done by the National Competent Authority (including an adjudicator and an authorised officer) in the performance or purported performance of a function under this Act, to the National Competent Authority (including an adjudicator and an authorised officer) concerned, and

(b) to any other person specified for that purpose by order of the Court.

(10)The Court may—

(a) on the consent of all of the parties, or

(b) where there is good and sufficient reason for so doing and it is just and equitable in all the circumstances,

treat the application for leave as if it were the hearing of the application for judicial review and may for that purpose adjourn the hearing on such terms as it may direct.

(11)The Court shall not grant leave under this section unless it is satisfied that—

(a) there are substantial grounds for contending that the decision or act concerned is invalid or ought to be quashed,

(b) the applicant is materially affected by or has a sufficient interest in the matter which is the subject of the application, and

(c) the matter does not relate to a decision by an adjudicator under Head 44AC or 44AD.

(12)If the court grants leave under this section, no grounds shall be relied upon in the application for judicial review under Order 84 other than those determined by the Court to be substantial under subsection (11)(a).

(13)The Court may, as a condition for granting leave under this section, require the applicant for such leave to give an undertaking as to damages.

(14)If an application is made for judicial review under Order 84 in respect of part only of a decision or other act to which subsection (1) applies, the Court may, if it thinks fit, declare to be invalid or quash the part concerned or any provision thereof without declaring invalid or quashing the remainder of the decision or other act or part of the decision or other act, and if the Court does so, it may make any consequential amendments to the remainder of the decision or other act or the part thereof that it considers appropriate.

(15)The Court shall, in determining an application under this section or an application for judicial review on foot of such leave—

(a) act as expeditiously as possible consistent with the administration of justice, and

(b) give such priority as it reasonably can, having regard to all the circumstances, to the disposal of proceedings in that Court under this section.

Explanatory Note

This Head establishes that the validity of a decision made or an act done by the NCA in the performance of a function under Part 6 or Chapters 1 to 7 of this Part shall not be challenged other than by way of an application for judicial review, or in accordance with a process provided for in this Act by which the validity of such decision or act may be challenged.

Head 44AT- Appeals to Court of Appeal

(1) An appeal to the Court of Appeal shall lie in respect of a determination of the High Court on an appeal under Head 44AO in respect of a decision by an adjudicator under Head 44AC or 44AD.

(2) The determination of the High Court on—

(a) an application for confirmation under Head 44AR ,

(b) an application for judicial review of any other decision made or act done under this Act by the National Competent Authority (including decisions made or acts done under this Act by an authorised officer or by an adjudicator),

(c) a reference to the Court by way of case-stated by an adjudicator under Head 44AT ,

shall be final and no appeal shall lie from the decision of the High Court to the Court of Appeal in any case save with leave of the High Court, which leave shall only be granted where the High Court certifies that its decision involves a point of law of exceptional public importance and that it is desirable in the public interest that an appeal should be made to the Court of Appeal.

(3) In respect of an application for confirmation under Head 44AR , where the point of law which would otherwise be certified is a point that could have been brought by way of an appeal under Head 44AS , the High Court may only in exceptional circumstances grant leave to appeal to the Court of Appeal under subsection (2).

(4) Subsection (2) shall not apply to a determination of the High Court in so far as it involves a question as to the validity of any law having regard to the provisions of the Constitution.

(5) On an appeal from a determination of the High Court to which subsection (2) applies, the Court of Appeal shall—

(a) have jurisdiction to determine only the point of law certified by the High Court under subsection (2) (and to make only such order in the proceedings as follows from such determination), and

(b) in determining the appeal, act as expeditiously as possible consistent with the administration of justice.

Explanatory Note

This Head states, amongst other things, that an appeal to the Court of Appeal shall lie in respect of a determination of the High Court on an appeal under Head 44AP in respect of a decision by an adjudicator under Head 44AC or 44AD. Such appeals will only be granted with leave of the High

Court and where the High Court certifies that the decision involves a point of law of exceptional public importance and that it is desirable in the public interest that an appeal should be made to the Court of Appeal.

Head 44AU- Treatment of amounts paid to National Competent Authority pursuant to Part 8A

A payment received by the National Competent Authority of any amount due to it pursuant to this Part shall be paid into, or disposed of for the benefit of, the Exchequer in such manner as the Minister for Finance may direct.

Explanatory Note

This Head provides that a payment received by the NCA of any amount due to it pursuant to this Part shall be paid into, or disposed of for the benefit of, the Exchequer in such manner as the Minister for Finance may direct.

Head 44AV- National Competent Authority to collect information relating to appeals and decisions to grant interim measures

1) The National Competent Authority shall collect information on the general subject matter of appeals under this Chapter, the number of appeals and the duration of appeal proceedings and the number of decisions to grant urgent interim measures.
2) The information collected by the National Competent Authority under subsection (1) shall be provided to the Minister annually or as requested by the Minister.

Explanatory Note

This Head provides that the NCA shall collect information on the general subject matter of appeals under this Chapter, the number of appeals, the duration of appeal proceedings and the number of decisions to urgent interim measures; and provide this information to the Minister.

Part 9- Final Provisions

Head 45- Amendments to other Legislation by Directive (EU) 2022/2555

(1) The Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 will require amendment or potentially sign posting from this [Act] back to the relevant sections in the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, as the NIS2 Directive goes beyond what is provides for some of the same provisions.

Explanatory Note:

Article 43 of the DIRECTIVE (EU) 2022/2555 (NIS2) deletes Articles 40 and 41 of Directive (EU) 2018/1972.

- DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code (EECC)
    - Article 40 - Security of networks and services
    - Article 41 - Implementation and enforcement

Primary legislation giving effect to the transposition of the EECC, is the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023. DECC is the Department responsible for this legislation. The Regulatory Authority is ComReg.

The Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 will require amendment or the repeal of the relevant sections (and replaced within the NIS2 Bill). Where the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 only applies to providers of public electronic communications networks of publicly available electronic communications services and Directive (EU) 2022/2555 (NIS2) applies more generally to essential entities, the 2023 Act could retain a cross reference to the new Bill to indicate that telecoms companies are essential entities for the purpose of the NIS2 Bill, which would ensure the new Bill is read alongside the 2023 Act.

The transposition table of the EECC points the following sections of the Communications Regulations and Digital Hub (Amendment) Act transpose Articles 40 and 41: Section 5 (general definitions), Art 40.1 given effect to by s6 (1)-(3), Art 40.2 by section 11, Art 40.3 by s12, Art 41.1, 41.2 and 41.3 by sections 13 and 14 and Article 41.4 and 41.5 by section 16 – it would appear to me that the provisions of the Act would be repealed, but the relevant provisions of NIS2 could be given effect to in the Bill by amending these sections, that really depends on where the new provisions sit best Under NIS2, Public Electronic Communications Networks are deemed to be an Essential entity. Therefore, the provisions of Art 40 of DIRECTIVE (EU) 2018/1972 would correspond with those of Article 21 (Cybersecurity Risk-Management Measures) and Article 23 (Reporting Obligations) in NIS2.

The provisions of Art 41 of DIRECTIVE (EU) 2018/1972 would correspond with those of Article 31(General aspects concerning supervisions and enforcement) and Article 32 (Supervisory and enforcement measures in relation to essential entities).

However, in both cases the provisions in NIS2 go beyond what is provided for in DIRECTIVE (EU) 2018/1972. It should also be noted there are no conflicts of policy regarding the implementation of the two Directives. These provisions are in the main for a drafter to consider on how best to address.

Head 46 – Amendment to The Communications Regulation Act 2002

Commission for Communications Regulation (COMREG)

"The Communications Regulation Act 2002 is amended—

in section 30—

(i) by inserting after subsection (2) the following:

"(2B) For the purpose of meeting expenses properly incurred by the Commission in the discharge of its function in relation to the Critical Entities Resilience Directive (Directive (EU) 2022/2557), the Commission may make an order imposing a levy on Digital Infrastructure providers.",

(ii) in subsection (3) by inserting "or the Critical Entities Resilience Directive (Directive (EU) 2022/2557)" after "electronic communications services",

(iii) by substituting for subsection (11) the following:

"(11) The Commission shall not impose a levy on providers of—

(a) electronic communications for the purpose of meeting expenses properly incurred by the Commission in the discharge of its functions in respect of postal services or premium rate services or the Critical Entities Resilience Directive (Directive (EU) 2022/2557),

(b) postal services for the purpose of meeting expenses properly incurred by the Commission in the discharge of its functions in respect of electronic communications services or premium rate services or the Critical Entities Resilience Directive (Directive (EU) 2022/2557), or

(c) premium rate services for the purposes of meeting expenses properly incurred by the Commission in the discharge of its functions in respect of postal services or electronic communications services or the Critical Entities Resilience Directive (Directive (EU) 2022/2557), or

(d) the Critical Entities Resilience Directive (Directive (EU) 2022/2557) for the purposes of meeting expenses properly incurred by the Commission in the discharge of its functions in respect of postal services or electronic communications services or premium rate services or the Network and information Systems Directive (Directive (EU) 2022/2555)."

Explanatory Note:
This Head amends the Communications Regulation Act 2002 to allow ComReg as a Competent Authority under the Directive to extend it levy funding activities to its functions under the CER Directive.

Head 47 – Amendment to section 33AK of Central Bank Act 1942

(1) Section 33AK(5) of the Central Bank Act 1942 (No. 22 of 1942) is amended—"

(a) in paragraph (bb) (amended by Regulation 57(a)(i)(II) of the European Union (Capital Requirements) (Amendment) Regulations 2020 (S.I. No 710 of 2020)) by substituting "and 2013/36/EU), or" for "and 2013/36/EU).", and

(b) by inserting the following paragraph after paragraph (bb):

(bc) with the bodies designated as the competent authorities in the State for the purposes of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC and

(bd) with the bodies designated as the competent authorities in the State for the purposes of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).".

Explanatory Note:
This Head relates to amendment to the Central Bank Act 1942 to allows the Central Bank of Ireland, to share information with other Competent Authorities, the NCSC etc, in line with their functions as a competent authority under the CER and NIS2 Directive. While there are other provisions in this [Act] to allow the Competent Authorities to share information, by amending the Central Bank Act there will be legal lacuna, especially as Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA) will be considered *Lex Specialis* when it comes into effect in January 2025.

Head 48- Amendment of the Communications (Retention of Data) Act 2011

To provide that:

The Communications (Retention of Data) Act 2011 is amended as follows:

(1) For the addition in section 1 of the following definition:

(a) "superior officer" means in relation to an officer of the National Cyber Security Centre, an officer not below the rank of Principal Officer.

(3) To insert in section 6 a new subsection (4A) as follows:

"(4A) A superior officer of the National Cyber Security Centre may require a service provider to disclose to that officer user data in the possession or control of the service provider -

(a) where the Superior Officer believes that the data relates to an incident whom the officer suspects, on reasonable grounds, of presenting an actual or potential threat to the security of network and information systems in the State, or

(b) where the Superior Officer has reasonable grounds for believing that the data are otherwise required for the purpose of preventing, detecting or investigating a risk to the security of network and information systems in the State."

(4) To insert in section 6C a new subsection (4A) as follows:

(4A) An officer of the NCSC not below the rank of Assistant Principal officer may apply to an authorising judge for an authorisation under this section where the officer is of the belief that the internet source data in respect of which the application is made –

(a) relate to an incident or risk to the security of network and information systems in the State

(b) are otherwise required to be preserved for the purpose of preventing, detecting or investigating a network and information security incident.

(5) To amend subsection (6) to delete "subsections (1), (2), (3) or (4)," and replace it with " subsections (1), (2), (3), (4) (4a) or (4b),".

(5) To insert in section 6D a new subsection (4c) as follows:

“(a) “(4c) Subject to subsection (15) an officer of the NCSC not below the rank of Assistant Principal officer may apply to a superior officer for an authorisation under this section where the officer believes on reasonable grounds that –

(a) paragraph (a) or (b) of section 6C(4b) apply to the internet source data in respect of which the application is made, and

(b) It is likely that, before the internet source data could be obtained pursuant to an authorisation under section 6C –

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the prevention, detection, of a network and information security incident would be impeded.”

and

(b) To amend subsection (5) as follows:

To delete “subsection (1), (2), (3) (4) or (4a),” and replace it with. subsection (1), (2), (3) (4), (4a) or (4b),”

(c) To amend subsection (10) by inserting subsection (f) as follows:

“(e) in relation to an authorisation pursuant to an application under subsection (4A), be submitted by the superior officer concerned to an officer of the NCSC not below the rank of Director.”

(11) By amending section 9 to include a new subsection (3C) as follows:

(a) “(3C) The NCSC shall prepare and submit a report to the Minister for Environment, Climate and Communications in respect of data specified in Schedule 2 that were the subject of all disclosure requirements made under section 6(4B), 6F(1), 7C or 7D during the relevant period.”;

(b) by amending subsection (4) to delete “or (3A) or (3B)” and replace it with “ (3A), (3B) or (3C)”

(c) by inserting a new subsection (7C) as follows:

“(7C Department for Environment, Climate and Communications) shall review the report submitted under subsection (3C) and shall forward it to the Minister, along with any comments that he or she may have with respect to it.”;

(12) By amending section 12G(1) to include after “ “ the Chairperson of the Corporate Enforcement Authority or where there is only Superior Officer of the Authority, the CEO and sole appointed Superior Officer of the Authority“, “the Director of the NCSC”.

Explanatory Note:
Amending the Communications (Retention of Data) Act 2011 (as amended by Communications (Retention of Data) (Amendment) Act 2022). This head seeks to amend the Criminal Justice (Retention of Data) Act 2011 to enable the NCSC to seek data relating to cyber security incidents and to align its powers with those of other enforcement agencies

like the Competition and Consumer Protection Commission and the Competition and the Corporate Enforcement Agency.

Further drafting and definitions will need to be provided for to ensure clarity of this Head to amend the Communications (Retention of Data) Act 2011, as the Act is currently being amended.

Head 49 Revoke S.I. 360 of 2018

(1) S.I. 360 of 2018 shall be revoked from the date this legislation comes into effect in the State.

Explanatory Note:
This Head relates to Article 44 of the DIRECTIVE (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union which repeals Directive (EU) 2016/1148 with effect from 18 October 2024. Directive (EU) 2016/1148 was transposed into Irish law by S.I. 360 of 2018 European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018. As the Department intends on commencing this [Act] all at once, the S.I. should only be revoked when this Bill is enacted to ensure there are no legislative gaps or lacuna. It is not expected any transitional provisions may be required.

Part 10 - Schedules

Schedule I - Sectors Of High Criticality

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council ([1]), which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive
		— Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944
		— Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944
		— Producers as defined in Article 2, point (38), of Directive (EU) 2019/944
		— Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council ([2]) — Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944 — Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
	(b) District heating and cooling	— Operators of district heating or district cooling as defined in Article 2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council ([3])
	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		— Central stockholding entities as defined in Article 2, point (f), of Council Directive 2009/119/EC ([4])
	(d) Gas	— Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parliament and of the Council ([5])
		— Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC

		— Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC
		— Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC
		— LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC
		— Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities
	(e) Hydrogen	— Operators of hydrogen production, storage and transmission

Sector	Subsector	Type of entity
2.Transport	(a) Air	— Air carriers as defined in Article 3, point (4), of [Act] (EC) No 300/2008 used for commercial purposes
		— Airport managing bodies as defined in Article 2, point (2), of Directive 2009/12/EC of the European Parliament and of the Council ([6]), airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to [Act] (EU) No 1315/2013 of the European Parliament and of the Council ([7]), and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of [Act] (EC) No 549/2004 of the European Parliament and of the Council ([8])
	(b) Rail	— Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council ([9])
		— Railway undertakings as defined in Article 3, point (1), of Directive 2012/34/EU, including operators of service facilities as defined in Article 3, point (12), of that Directive
	(c) Water	— Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to [Act] (EC) No 725/2004 of the European Parliament and of the Council ([10]), not including the individual vessels operated by those companies

		— Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC of the European Parliament and of the Council ([11]), including their port facilities as defined in Article 2, point (11), of [Act] (EC) No 725/2004, and entities operating works and equipment contained within ports
		— Operators of vessel traffic services (VTS) as defined in Article 3, point (o), of Directive 2002/59/EC of the European Parliament and of the Council ([12])
	(d) Road	— Road authorities as defined in Article 2, point (12), of Commission Delegated [Act] (EU) 2015/962 ([13]) responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity
		— Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council ([14])
3.Banking		Credit institutions as defined in Article 4, point (1), of [Act] (EU) No 575/2013 of the European Parliament and of the Council ([15])
4.Financial market infrastructures		— Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU of the European Parliament and of the Coun- cil ([16])
		— Central counterparties (CCPs) as defined in Article 2, point (1), of [Act] (EU) No 648/2012 of the European Parliament and of the Council ([17])

Sector	Subsector	Type of entity
5.Health		— Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council ([18])
		— EU reference laboratories referred to in Article 15 of [Act] (EU) 2022/2371 of the European Parliament and of the Council ([19])

		— Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council ([20]) — Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 — Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list) within the meaning of Article 22 of [Act] (EU) 2022/123 of the European Parliament and of the Council ([21])
6.Drinking water		Suppliers and distributors of water intended for human consumption as defined in Article 2, point (1)(a), of Directive (EU) 2020/2184 of the European Parliament and of the Council ([22]), excluding distributors for which distribution of water for human consumption is a non- essential part of their general activity of distributing other commodities and goods
7.Waste water		Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2, points (1), (2) and (3), of Council Directive 91/271/EEC ([23]), excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity
8.Digital infrastructure		— Internet Exchange Point providers
		— DNS service providers, excluding operators of root name servers
		— TLD name registries
		— Cloud computing service providers
		— Data centre service providers
		— Content delivery network providers
		— Trust service providers
		— Providers of public electronic communications networks
		— Providers of publicly available electronic communications services
9.ICT service management (business-to-business)		— Managed service providers — Managed security service providers

Sector	Subsector	Type of entity
10. Public administration		— Public administration entities of central governments as defined by a Member State in accordance with national law
		— Public administration entities at regional level as defined by a Member State in accordance with national law
11. Space		Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

(1) Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).

(2) [Act] (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).

(3) Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).

(4) Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9).

(5) Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211,
14.8.2009, p. 94).

(6) Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).

(7) Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).

(8) Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96,
31.3.2004, p. 1).

(9) Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32).

(10) Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).

(11) Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

(12) Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).

(13) Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real- time traffic information services (OJ L 157, 23.6.2015, p. 21).

(14) Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

(15) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176,
27.6.2013, p. 1).

(16) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173,
12.6.2014, p. 349).

(17) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

(18) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(19) Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26).

(20) Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).

(21) Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1).

(22) Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (OJ L 435, 23.12.2020, p. 1).

(23) Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p. 40).

Explanatory Note:
Schedule I transposes Annex I (SECTORS OF HIGH CRITICALITY) of the DIRECTIVE (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. The Schedule will be tailored to reflect the State context.

Schedule II- Other Critical Sectors

Sector	Subsector	Type of entity
1. Postal and courier services		Postal service providers as defined in Article 2, point (1a), of Directive 97/67/EC, including providers of courier services
2. Waste management		Undertakings carrying out waste management as defined in Article 3, point (9), of Directive 2008/98/EC of the European Parliament and of the Council ([1]), excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, as referred to in Article 3, points (9) and (14), of Regulation (EC) No 1907/2006 of the European Parliament and of the Council ([2]) and undertakings carrying out the production of articles, as defined in Article 3, point (3), of that Regulation, from substances or mixtures
4. Production, processing and distribution of food		Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council ([3]) which are engaged in wholesale distribution and industrial production and processing
5. Manufacturing	(a) Manufacture of medical devices and *in vitro* diagnostic medical devices	Entities manufacturing medical devices as defined in Article 2, point (1), of Regulation (EU) 2017/745 of the European Parliament and of the Council ([4]), and entities manufacturing *in vitro* diagnostic medical devices as defined in Article 2, point (2), of Regulation (EU) 2017/746 of the European Parliament and of the Council ([5]) with the exception of entities manufacturing medical devices referred to in Annex I, point 5, fifth indent, of this Directive
	(b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2

	(d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
	(f) Manufacture of other transport equipment	Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2
Sector	Subsector	Type of entity
6. Digital providers		— Providers of online marketplaces
		— Providers of online search engines
		— Providers of social networking services platforms
7. Research		Research organisations

(1) Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3).

(2) Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).

(3) Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p. 1).

(4) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

(5) Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

Explanatory Note:
Schedule II transposes Annex II (OTHER CRITICAL SECTORS) of the DIRECTIVE (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. The Schedule will be tailored to reflect the State context.